NÄRPES STAD
NÄRPIÖN KAUPUNKI

INFORMATIONSSÄKERHETSPOLICY FÖR NÄRPES STAD

Skapat datum: 29.10 2020
Dokumentansvarig: Informationssäkerhetsgruppen
Godkänd av: Stadsstyrelsen 16.12 2020

Innehållsförteckning

1. Inledning och bakgrund

Denna informationssäkerhetspolicy gäller för informationssäkerhet inom Närpes stad, och kompletterar stadens övriga styrdokument inom bland annat IT, kvalitet, kommunikation och övrig riskhantering. Denna policy gäller alla de arbetstagare, tjänsteinnehavare, förtroendevalda och representanter för intressentgrupper som inom ramen för sitt arbete eller uppdrag behandlar information som Närpes stad äger eller förvaltar.

Information är en mycket viktig resurs och en förutsättning för Närpes stad för att kunna bedriva en ändamålsenlig verksamhet. Informationen är inte sällan känslig om den sprids till obehöriga, bland annat med hänsyn till enskildas personliga integritet samt att information kan missbrukas för att störa samhällets funktionalitet eller för att tillskansa sig ekonomiska fördelar.

2. Syfte

Denna policy har som syfte att tydliggöra vad som krävs för säker informationshantering inom Närpes stads nämnder och bolag. Kontinuerligt informationssäkerhetsarbete är nödvändigt för att kunna uppfylla stadens uppdrag och mål. Syftet med informationssäkerhetsarbetet är att skydda stadens verksamhet mot avbrott och minska skador genom att förebygga och minimera verkan av oönskade händelser.

3. Informationssäkerhet

Den tekniska utvecklingen medför även att allt mer information lagras i molntjänster istället för på lokala servrar eller i fysisk pappersform. Denna utveckling innebär att kraven blir fler och större för hur information både behandlas och säkerställs. Närpes stad arbetar aktivt för att upprätthålla nödvändiga säkerhetskrav och för att garantera en informationssäker hantering inom verksamheten.

Informationssäkerhetspolicyn omfattar all sorts information, oavsett om det är information i molntjänster, i datorer, i telefonsamtal/sms, fysiska samtal eller på papper så gäller följande riktlinjer för hantering.

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån fyra aspekter:

- **Konfidentialitet**: att information inte tillgängliggörs eller avslöjas till obehörig
- **Riktighet**: att information är korrekt, aktuell och fullständig
- **Tillgänglighet**: att information är åtkomlig och användbar av behörig
- **Spårbarhet**: att informationsbearbetning ska kunna härledas till vem och när.

Information har i olika grad krav på sig gällande de fyra aspekterna. Kraven kan härledas från rättsliga krav eller från Närpes stads egna målsättningar. Dessutom har självklart invånare, företag och andra aktörer i vår omvärld, behov och förväntningar som ställer krav på vår informationssäkerhet.

Informationssäkerheten i Närpes stad omfattar även cybersäkerhet, dataskydd och andra delområden inom säkerhet. De mest centrala av dessa för staden är följande:

- Tryggande av konfidentialitet, integritet, tillgänglighet och kontinuitet i cyberrymden.
- Lagstadgat säkerställande av individens integritetsskydd och rättigheter som tryggar detta vid

behandling av personuppgifter.
- Skydd av stadens lokaler och människorna, informationen och annan egendom som finns där mot skador av olika slag, mot försök till skadegörelse och mot obehöriga personer.
- Åtgärder i personalprocessen innan anställningsförhållandet inleds, medan det pågår och när det upphör.

4. Mål

Informationssäkerhet har inget egenvärde, utan ska bidra till att Närpes stad når sina övergripande visioner, strategier och mål. Närpes stad ska uppnå och upprätthålla en informationssäkerhet som

- innebär en robust, säker och tillförlitlig informationshantering,
- möjliggör ett aktivt medverkande i det digitala samhället,
- bidrar till att uppsatta mål nås gällande exempelvis kvalitet, effektivitet och personlig integritet,
- motsvarar invånares och externa verksamheters behov och förväntningar,
- uttrycks i aktuella styrdokument som policy och riktlinjer,
- efterlever krav i lagar, förordningar, föreskrifter och avtal.

5. Organisering, roller och ansvar

Alla som i någon utsträckning hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Ansvaret för respektive verksamhets informationssäkerhet följer verksamhetsansvaret. Närpes stads policy för informationssäkerhet antas av stadsstyrelsen.

Informationshanteringsenheten (stadsstyrelsen) följer upp informationssäkerheten i staden. Stadsstyrelsen godkänner informationssäkerhetspolicyn, anvisningar och riktlinjer som gäller hela staden. Stadsstyrelsen ordnar den interna kontrollen och riskhanteringen.

Informationssäkerhetsansvarige (stadsdirektören) har ett helhetsansvar för informationssäkerheten och rapporteringen om denna till stadsstyrelsen. Informationssäkerhetsansvarige ansvarar för informationssäkerhetspolicyn och föredrar ändringarna för stadsstyrelsen. Stadens ledningsgrupp och informationssäkerhetsgruppen bistår stadsdirektören i frågor som gäller informationssäkerhet.

Informationssäkerhetsgruppen följer med informationssäkerhetens allmänna utveckling och hotbilder samt följer upp informationssäkerhetsarbetet i staden. Gruppen analyserar och utvärderar den ovan nämnda helheten och ger utifrån utvärderingen förslag till förbättring av informationssäkerheten. Dessutom bistår gruppen hela stadens förvaltning i frågor som gäller informationssäkerhet.

Sektordirektörerna svarar för riskhantering och beredskap samt informationssäkerheten och dataskyddet inom sina sektorer.

Styrelserna och de verkställande direktörerna för stadens koncernbolag svarar för informationssäkerheten och dataskyddet inom sina organisationer.

Områdescheferna och förmännen svarar för informationssäkerheten inom sitt ansvarsområde.
Deras viktigaste uppgifter är att se till:

- att de anställda introduceras i stadens informationssäkerhets- och dataskyddsanvisningar och

det ansvar som hör till varje anställd,

- när en anställds anställningsförhållande upphör eller när personen övergår till andra uppgifter, att stadens information och övriga egendom återlämnas och att IT-personal / Dynamo Net informeras så att de kan avlägsna behörigheter.

Personalen svarar för att följa anvisningarna. Var och en ska dessutom omedelbart anmäla om avvikelser, hot och risker som gäller informationssäkerhet till datasäkerhetsansvarige och dataskyddsansvarige eller till sin chef.

Den som ”äger” informationen svarar för klassificering av informationen (offentlighet och sekretess) och säkerställande av dess integritet samt sparande av informationen enligt klassificeringen.

”Ägaren” till ett dataprogram svarar för riskhantering av och beredskap för störningar i programmet och informationen i detta samt för informationssäkerheten. Behörighet beviljas på ansökan av den anställdas förman av ägaren till dataprogrammet eller den som denne befullmäktigat.

”**Ägaren” till en process** svarar för riskhantering av och beredskap för störningar i processen samt för informationssäkerheten. Han eller hon svarar också för identifiering av processens beroendeförhållanden och bedömning av hur kritiska dessa är.

IT-säkerhetsansvarige svarar för IT-säkerheten, beredningen av riktlinjer som stöder denna och för att IT-säkerhetskraven efterlevs. IT-säkerhetsansvarige följer upp IT-säkerheten inom staden och rapporterar om tillgodoseendet av denna till informationssäkerhetsansvarige och informationssäkerhetsgruppen.

Dataskyddsansvarige svarar för dataskyddet, beredningen av riktlinjer som stöder detta och för att kraven och lagarna gällande dataskydd efterlevs. Dataskyddsansvarige följer upp dataskyddet inom staden och rapporterar om tillgodoseendet av denna till informationssäkerhetsansvarige och dataskyddsgruppen.

Dataskyddsombudet är en organisationsintern sakkunnig, som följer behandlingen av personuppgifter och ger hjälp vad gäller efterlevnaden av dataskyddsbestämmelserna i hela organisationen och koncernbolagen. Fungerar även som kontaktperson för invånarna, personalen och dataombudsmannens byrå i frågor gällande personuppgiftsbehandling och dataskydd.

Datasskyddsgruppen består av kontaktpersoner inom dataskydd. Gruppen sammanträder regelbundet samt alltid vid behov för att behandla dataskyddsärenden. Dataskyddsgruppens uppgift är att sörja för att ansvarsskyldigheten uppfylls, utarbeta en dataskyddspolicy, koordinera personalens utbildning samt att övervaka dataskyddets förverkligande som helhet.

Dokumentförvaltningen svarar för dokumenthanteringen och anvisningarna som gäller denna. Interna revisionen svarar för att informationssäkerheten är ändamålsenlig och för utvärderingen av om den är tillräcklig samt för revision.

Personalförvaltningen svarar för informationssäkerheten och dataskyddet i personalprocessen. Detta ansvar omfattar:

- anvisningar och stöd till personalen
- ordnande av utbildning och introduktion i informationssäkerhet och dataskydd
- kontroll av bakgrundsuppgifter vid behov.

Stadsarkivet har tillsynsansvar för att informationen hanteras enligt bestämmelserna i kommunallagen, förvaltningslagen, arkivlagen och offentlighets- och sekretesslagen, samt kommunens interna styrdokument rörande informationens långsiktiga hantering och bevarande.

Personuppgiftsansvariga är stadsstyrelsen och övriga nämnder inom staden.
Dessa är ansvariga för hanteringen av personuppgifter och ska kontrollera att personuppgifter hanteras på ett korrekt sätt i verksamheten.

6. Informationsklassning

Stadens informationstillgångar ska klassificeras med hänsyn till krav på konfidentialitet, riktighet, spårbarhet och tillgänglighet. Därigenom kan lämpliga skyddskrav ställas upp för respektive informationstillgång. För de tillgångar som bedöms vara särskilt viktiga ska riskanalyser och konsekvensbedömningar upprättas.

För de verksamhetssystem som i informationsklassificeringen konstateras vara kritiska för verksamheten ska en systemsäkerhetsplan upprättas och hållas uppdaterad. För informationstillgångar med höga krav på tillgänglighet inkluderar det en kontinuitetsplan.

7. Principer för arbetet

Närpes stad ska arbeta med informationssäkerhet på ett sätt så att ovanstående mål uppfylls. Arbetet med informationssäkerhet ska gentemot stadens verksamheter vara normerande, stödjande och kontrollerande. Viktiga förmågor i det arbetet är att kunna identifiera hot, sårbarheter och risker rörande Närpes stads informationstillgångar samt att kunna utforma och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå.

Arbetet med informationssäkerhet inom Närpes stad ska:

- bygga på en helhetssyn som utgår från information, men som också innefattar processer, människor och teknik,
- löpande ses över och förbättras, eftersom Närpes stad och dess omvärld, inklusive hotbild, är under ständig förändring,
- vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter allvarliga störningar och kriser som ändå kan inträffa,
- bygga på Närpes stads värderingar och ta hänsyn till verksamheters behov, externa krav samt rådande hotbild,
- vara väl kommunicerat till verksamheten; all personal ska fortlöpande få information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande och för att kunna leva upp till denna policy och underliggande riktlinjer för informationssäkerhet,
- ske i aktiv samverkan med det omgivande samhället såsom myndigheter, företag och nätverk,
- ska beaktas vid anskaffning, utveckling och avveckling av datasystem

8. Revidering, uppföljning och rapportering

Informationssäkerhetspolicyn revideras vid behov och ansvarig för detta är stadens informationssäkerhetsgrupp. Efterlevnaden av informationssäkerhetspolicyn och riktlinjer för informationssäkerhet ska följas upp regelbundet.

IT-säkerhetsansvarige ska på begäran rapportera läge och status gällande IT-säkerhet till informationssäkerhetsansvarige och informationssäkerhetsgruppen. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, skall alltid rapporteras.

Dataskyddsansvarige ska på begäran rapportera läge och status gällande dataskydd till informationssäkerhetsansvarige och informationssäkerhetsgruppen. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, skall alltid rapporteras.