Utgivare: Kommunledningskontoret
Gäller från: 2004-04-01
Antagen: KF § 47/2004

Policy för IT-säkerhet i Ronneby kommun

Avsikten med denna policy är att skapa ett gemensamt synsätt så att målet för säkerhetsarbetet blir lika inom Ronneby kommunkoncern.[1]

Med IT-säkerhet avses de säkerhetsåtgärder som krävs för att skydda information och den teknik som används för att hantera informationen.

Information och data är en av verksamheternas viktigaste resurser och representerar stora värden. IT-säkerhet krävs för att bibehålla och utöka medborgarnas förtroende när information hanteras. Fel och brister kan orsaka stor skada.

1. Mål för IT-säkerhetsarbetet

Målet med IT-säkerhetsarbetet är att skydda information. Skyddet avser intrång, stöld, avlyssning, skadegörelse, driftavbrott, fysisk skada eller annan åverkan. Den kommunala verksamheten ska vara säkerställd, och därmed den service kommunen erbjuder medborgarna. Hänsyn ska tas till de lagar och förordningar som direkt påverkar respektive verksamhet.

Policyn tillsammans med gällande regler och riktlinjer för IT-säkerhet syftar till att säkerställa sekretess, tillgänglighet, riktighet och spårbarhet för information och data samt att reducera risken för skador.

2. Säkerhetsarbetets omfattning

IT-säkerhetsarbetet omfattar all form av information som bearbetas och lagras elektroniskt.

IT-säkerhetsarbetet innebär att risk- och sårbarhetsanalyser ska genomföras i befintliga system samt vid anskaffning eller större förändring av datorstöd. Analyserna ska dokumenteras och förvaras säkert.

Säkerhetsnivån ska stå i relation till bedömda hot, risker och konsekvenser. Hoten kan vara externa eller interna, avsiktliga eller oavsiktliga. Skyddsåtgärder ska vara risk- och lönsamhetsmässigt rimliga i förhållande till informationens och systemens värde. Säkerhetsnivån ska regelbundet kontrolleras gentemot införda skyddsåtgärder och resultat från riskanalyser.

[1] Med Ronneby kommun avses kommunkoncernen d.v.s. omfattar samtliga verksamheter, bolag och annan organiserad verksamhet där kommunen har ett dominerande inflytande.

3. Ansvar - organisation

3.1. Övergripande ansvar

Kommunstyrelsen har det övergripande ansvaret för IT-säkerhet och att fatta beslut om regler och anvisningar för IT-säkerhetsarbetet.

Varje nämnd eller bolagsstyrelse ska inom sitt område se till att verksamheten bedrivs i enlighet med denna policy och fastställda regler och riktlinjer. Nämnden respektive bolagsstyrelsen ska även se till att erforderliga resurser ställs till förfogande för säkerhetsarbetet så att kraven på säkerhet uppfylls.

Nämnder och styrelser ansvarar för att IT-systemen i deras verksamhet uppfyller kraven på säkerhet.

Kostnader för IT-säkerhetsåtgärder ska ingå i respektive verksamhets budget.

3.2. Samordningsansvar

Kommundirektören ansvarar ytterst för att säkerhetsarbete genomförs i erforderlig omfattning. För det praktiska samordningsarbetet av IT-säkerheten ansvarar dock särskilt utsedd samordnare, d.v.s. säkerhetssamordnare med samordningsansvar för IT-säkerhet (i det följande benämnd säkerhetssamordnare).

För genomförande av säkerhetsarbetet har kommundirektören möjlighet att tillsätta en arbetsgrupp med uppgift att medverka i samordningsarbetet. Gruppens sammansättning beslutas av kommundirektören.

3.3. Beslut om genomförande av säkerhetsåtgärder

Beslut om säkerhetsåtgärder fattas i första hand av Kommundirektören inom de ramar som meddelas av Kommunstyrelsen. Kommundirektören har rätt till vidaredelegation. För sådan vidaredelegation ska de formella rutiner som gäller för delegation iakttas.

3.4. Utbildning och information

Verksamhetschefen respektive bolagsdirektören ansvarar för att medarbetarna får den information och utbildning som krävs för god informationssäkerhet och högt säkerhetsmedvetande.

Ett aktivt, systematiskt och kontinuerligt IT-säkerhetsarbete ska bedrivas för att skydda information och informationssystem.

3.5. Uppföljning av policyns efterlevnad

Verksamhetschefen respektive bolagsdirektören ansvarar för att riskanalyser, skyddsåtgärder och utbildningsinsatser kontinuerligt följs upp.

3.6. Förteckningar, granskning och utvärdering

Liksom annan kommunal verksamhet ska IT-säkerheten regelbundet revideras.

Varje verksamhet ska föra register över programtillgångar och ha dokumenterade bevis för äganderätt till licenser.

Viktiga register och andra förteckningar inom verksamheterna ska skyddas mot avslöjande, förlust, förstörelse och förfalskning. För elektroniskt lagrat material ska rutiner upprättas som säkerställer läsbarheten under hela bevarandeperioden. Detta för att skydda mot förlust om tekniken ändras i framtiden.

Respektive verksamhetschef och bolagsdirektör ska se till att kontroll av att säkerhetsrutinerna inom deras ansvarsområden utförs korrekt och regelbunden granskning av efterlevnaden sker.

Informationssystemen ska regelbundet kontrolleras så att de uppfyller säkerhetsnormerna. I den tekniska kontrollen ingår att granska driftsystem för att säkerställa att styrmedel och säkerhetsåtgärder hos datorutrustning och program har införts korrekt. Sådana kontroller ska endast utföras av kompetent och behörig personal.

4. Information och utbildning

Ronneby kommunkoncern är beroende av ett IT-stöd som fungerar. Frågorna om IT-säkerhet måste uppmärksammas på ett systematiskt och strukturerat sätt. All personal bör vara informerad om betydelsen av IT-säkerhet och få den utbildning som de behöver.

Information om IT-säkerhet ska ingå i introduktionen vid nyanställning.

Varje anställd inom Ronneby kommunkoncern som arbetar inom sekretesskyddad verksamhet ska informeras om hantering av känslig och sekretessbelagd information.

Vid nyanställning eller vid byte av arbetsuppgifter ska information om IT-säkerhet lämnas. Frågor om IT-säkerhet och de förutsättningar som gäller för arbete med sekretessbelagd eller annan känslig information bör även uppmärksammas vid anlitande av konsulter, servicebyråer o.dyl.