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

Regler och riktlinjer för IT-säkerhet i Ronneby kommun

1. Allmänt

1.1. Begrepp

IT-säkerhet används i betydelsen att i första hand omfatta skydd av information som finns i Ronneby kommuns system och skydd av den teknik som hanterar informationen.

IT-säkerhet består av fyra grundkomponenter:
sekretess – säkerställa att information är tillgänglig endast för dem som har behörighet för åtkomst,
tillgänglighet – säkerställa att behöriga användare vid behov har tillgång till information och tillhörande tillgångar,
riktighet – skydda information och behandlingsmetoder så att de förblir korrekta och fullständiga,
spårbarhet – skydda från förluster och brott mot säkerheten, återställa om skada inträffar.

Vid analyser av IT-säkerhet förekommer följande definitioner:
Riskanalys: systematisk metod för att fastställa risk för system eller funktion.

Risk: konsekvensen av en händelse i förhållande till sannolikheten att den inträffar.
Hot: händelser och störningar som kan påverka verksamheten negativt.
Brist : svaghet som kan utgöra ett hot.
Sårbarhet : en svaghet som kan användas och därmed bli ett hot.
Konsekvens: effekten av ett hot som förverkligats.

"Regler och riktlinjer för IT-säkerhet i Ronneby kommun" grundar sig på standarden SS-ISO/IEC 17799 (Ledningssystem för informationssäkerhet).

1.2. Policy för IT-säkerhet i Ronneby kommun

Vid tillämpningen av "Regler och riktlinjer i Ronneby kommun" ska vad som anges i "Policy för IT-säkerhet i Ronneby kommun" beaktas.

2. Tillämpningsområde

"Regler och riktlinjer för IT-säkerhet i Ronneby kommun" ska tillämpas inom Ronneby kommunkoncern.[1]

Reglerna omfattar anskaffning, utveckling, förvaltning, drift samt avveckling av både IT-utrustning och tillämpningar.

3. Säkerhetsorganisation

3.1. Samordningsansvar

Kommundirektören ansvarar ytterst för att säkerhetsarbete genomförs i erforderlig omfattning.

3.2. Säkerhetssamordnarens uppgifter

Säkerhetssamordnaren ansvarar för det praktiska samordningsarbetet och för uppföljningen av säkerhetsarbetet. Ansvaret omfattar att

- att utarbeta regler och anvisningar för IT-säkerhetsarbetet och att hålla dessa aktuella,
- bevaka att IT-säkerheten följs vid upphandlingar av datorutrustning och programvaror,
- informera verksamhetsansvariga om IT-säkerhetsarbetet,
- ge råd och stöd i övergripande frågor och stimulera säkerhetsmedvetandet,
- granska IT-säkerhetsincidenter,
- bevaka att säkerhet ingår som ett led i IT-planeringen samt
- årligen rapportera till kommunstyrelsen om IT-säkerhetsarbete.

Situation kan uppstå där säkerhetssamordnarens uppgifter behöver utföras av annan. Om sådant behov uppstår och det bedöms nödvändigt fattas beslut om utförande av uppgift av Kommundirektören. Kommundirektören ansvarar för att sådana beslut rapporteras till kommunstyrelsens arbetsutskott.

3.3. IT-säkerhetsansvar inom respektive verksamhet och bolag

Respektive verksamhetschef och bolagsdirektör ansvarar för att säkerhetsansvarig utses inom dess verksamhet. Säkerhetsansvarig ansvarar för att

1. bevaka att gällande lagar m.m. och Ronneby kommuns bestämmelser som berör IT-säkerhetsområdet efterlevs,
2. upprätthålla systematiska och löpande kontroller av IT-säkerhetsnivån,
3. se till riskanalyser genomförs,
4. omedelbart rapportera säkerhetsincidenter till säkerhetssamordnaren,
5. klassificera IT-tillgångar,
6. genomföra beslutade säkerhetsåtgärder,
7. bevaka att rutiner för behörighetsadministration följs,

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

8. bevaka att regler och rutiner mot datavirus följs,
9. lämna årlig IT-säkerhetsrapport till säkerhetssamordnaren.

Alla användare är skyldiga att omedelbart rapportera befarade brister i IT-säkerheten till systemansvarig eller till säkerhetsansvarig inom verksamheten.

4. Utbildning och information

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

5. Redovisning av IT-tillgångar

5.1. Förteckningar, granskning och utvärdering

Varje verksamhet ska inom ordinarie inventarieförteckning redovisa IT-tillgångar. Hit hör mjukvaror, hårdvaror, databaser och register. Varje post ska ges en tydlig identitet.

Gemensamma databaser eller register ska ingå i förteckning för den verksamhet som äger systemet.

Varje verksamhet ska ha dokumenterade bevis för äganderätt till licenser.

6. Klassificering av information

Klassificering av information ska ske för att rätt skyddsåtgärder ska kunna vidtas. Speciella krav ställs på information som klassas som *sekretessbelagd* eller *känslig*. Skyddet hanteras dels genom behörighetskontroll, dels genom riktlinjer för hantering och skydd av informationen (se bilaga 1).

6.1. Sekretessbelagd och annan känslig information

Uppgifter som bedöms vara av sådant slag att de ska beläggas med sekretess eller är sekretessbelagda enligt sekretesslagen (1980:100) ska behandlas på särskilt sätt.

Sekretessbelagd information får endast vara tillgänglig för den som behöver den för att fullgöra sina arbetsuppgifter eller för den som har lagligt stöd att få tillgång till informationen.

Information med uppgifter som rör rikets säkerhet ska förvaras i säkerhetsskåp och får inte hanteras i kommunkoncernens datasystem.

6.2. Känslig information

Information kan vara känslig utan att vara sekretessbelagd och bör i så fall inte spridas. Särskild hänsyn ska tas till personuppgiftslagen (1998:204).

Information som i sig inte är sekretessbelagd eller känslig kan när den kombineras eller samkörs med andra register eller databaser bedömas skada enskilda eller allmänna intressen. Systemansvarig ska ta hänsyn till detta vid utdelning av behörighet.

Respektive verksamhetschef och bolagsdirektör ansvarar inom sitt ansvarsområde för att känslig och sekretessbelagd information skyddas på ett tillfredställande sätt.

6.3. Ansvar för skapad information

Den som skapar information är ansvarig för att den blir hanterad på rätt sätt och för att känslig och sekretessbelagd information inte lämnas ut till obehörig.

7. Personal och säkerhet

Vid nyanställning eller vid byte av arbetsuppgifter ska information om IT-säkerhet lämnas.

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

Vid uppdrag till konsulter, servicebyråer o.dyl ska i avtalen anges de förutsättningar som gäller för arbete med sekretessbelagd eller annan känslig information samt eventuella villkor som gäller i övrigt.

8. Hantering av säkerhetsincidenter och säkerhetsproblem

8.1. Rapportering

Incidenter som påverkar säkerheten ska rapporteras till ansvarig för IT-säkerheten inom respektive verksamhet. Incidenter ska dokumenteras och rapporteras vidare till säkerhetssamordnaren. Samordnaren rapporterar till Kommundirektören.

Följande incidenter ska rapporteras:

- dataintrång (portscanning, brandväggsintrång, intrång i behörighetskontrollsystem, flooding)

- datavirus eller andra skadliga program (virus, trojan, logisk bomb, sniffer)

- händelse som medför driftavbrott eller fysisk skada (stöld, brand, vatten, blixtnedslag, värme, sabotage).

8.2. Nyckelpersonsberoende

Inom varje verksamhet ska nyckelpersonsanalyser genomföras och dokumenteras. För samtliga nyckelpersoner ska ersättare vara utsedd och vid behov utbildas. Respektive verksamhetschef och bolagsdirektör ska aktivt verka för att beroendet av nyckelpersoner minskar.

9. Fysisk och miljörelaterad säkerhet

9.1. Skalskydd

System för informationsbehandling som är kritiska eller känsliga för verksamheten ska inrymmas i säkra utrymmen inom ett avgränsat skalskydd med lämpliga säkerhetsspärrar och tillträdeskontroller. Skyddets nivå ska stå i proportion till riskerna.

9.2. Skydd av utrustning

Datorutrustning ska ha en rimlig skyddsnivå. De säkerhetsåtgärder som vidtas ska vara anpassade till de hot och risker som finns.

Mobil och bärbar datorutrustning inklusive mobiltelefoner och handdatorer får inte lämnas obevakade.

Lokal för serverutrustning och televäxelutrustning ska ha högsta skyddsnivå. Tillträde ska vara kontrollerat och begränsat. Lokalen ska ha godkänt brand- och översvämningsskydd. För prioriterad utrustning ska reservkraft finnas. Utrymmen för korskopplingspunkter, switchar, etc. ska vara låsta.

9.3. Säkerhet för utrustning utanför egna lokaler

Verksamhetschef eller bolagsdirektör ska godkänna om IT-utrustning används utanför kommunkoncernens lokaler. Säkerheten ska vara likvärdig som för utrustning installerad inom de egna lokalerna.

Utrustning och media som medförs utanför organisationen får inte lämnas obevakad. Bärbara datorer ska medföras som handbagage och om möjligt döljas under resor.

9.4. Säker avveckling eller återanvändning av utrustning

Lagringsmedia som innehåller känslig eller sekretessbelagd information ska fysiskt förstöras och därefter skrotas.

Alla utrustningsenheter som har lagringsmedia t.ex. fasta hårddiskar ska kontrolleras innan utrustningen avvecklas. Detta för att säkerställa att data och licensierade program har tagits bort eller skrivits över.

10. Styrning av kommunikation och drift

10.1. Driftrutiner och driftansvar

Gemensamma register och databaser ska ha en informationsägare och ska finnas i en grundversion som uppdateras centralt.

Ansvar och rutiner för styrning och drift av all utrustning som behandlar elektronisk information ska vara fastställda och dokumenterade.

Ansvar och rutiner för incidenthantering ska vara dokumenterade. Dokumentation förvaras på respektive verksamhet.

För att öka driftsäkerheten på de lokala nätverken ska enhetliga maskinvaror eftersträvas. Inköp av maskinvara och anslutning till nätet ska ske i samråd med och efter godkännande av IT-enheten.

10.2. Systemplanering och systemgodkännande

Samråd ska ske med kommunens IT-arbetsgrupp innan nya system införs. Det samma gäller vid större förändringar av system.

Krav som driften av nya system ställer ska fastställas, dokumenteras och testas innan de godtas och tillämpas.

10.3. Skydd mot skadliga program

Ronneby kommunkoncern ska skydda sina tillgångar mot skadliga program. På alla persondatorer ska det finnas virustestprogram som uppgraderas regelbundet. Programvarorna ska vara godkända av IT-enheten.

Alla användare ska informeras och göras medvetna om de risker som finns med obehöriga och skadliga program.

10.4. Regler och rutiner för säkerhetskopiering

All väsentlig information i systemet ska kunna rekonstrueras med säkerhetskopior och återlagringsrutiner. Undantaget är den information som tillförts verksamhetssystemet efter senaste säkerhetskopiering.

Dokumenterade rutiner för säkerhetskopiering ska finnas för att säkerställa att information, program och system inte kan gå förlorade. Säkerhetskopior ska förvaras i för ändamålet avsedda utrymmen. Säkerhetskopierade data ska regelbundet testas för att säkerställa att de är återläsbara.

Central back-up utförs endast på filer lagrade på kommunägd server. Medarbetare som sparar information på annan plats än anvisad server, ansvarar för att informationen blir säkerhetskopierad.

10.5. Mediahantering och mediasäkerhet

Media eller utrustning som innehåller filer med känslig och sekretessbelagd information och som förvaras eller transporteras utanför kommunens lokaler (exempelvis filer på hårddisken i en laptop) ska kontinuerligt bevakas eller vara krypterade.

Verksamhetschef respektive bolagsdirektör ska godkänna allt arbete med känslig och sekretessbelagd information utanför arbetsplatsen.

Rutiner ska vara etablerade för hantering av känsliga data och sekretessbelagd information. Om innehållet är känsligt ska datamedier fysiskt förstöras innan de avyttras eller kasseras.

Systemdokumentation ska skyddas från obehörig åtkomst.

10.6. Utbyte av information och program

Allt utbyte av information, data och program mellan Ronneby kommunkoncern och andra organisationer ska styras av gällande lagar och andra författningar, avtal och eventuellt andra yttre säkerhetskrav. Säkerhetskontroller och ansvarsförhållanden ska specificeras.

10.7. Extern resurs

Med extern resurs avses utnyttjande av enskilda konsulter eller konsultföretag samt serviceföretag för datordrift.

All användning av konsulter och serviceföretag ska vara reglerad genom avtal.

Vid anlitande av extern personal som utför uppdrag för Ronneby kommun ska överenskommelse träffas att säkerhetsincidenter och upptäckta säkerhetsbrister ska rapportera till uppdragsgivaren.

SUA-avtal (säkerhetsskyddsavtal) ska tecknas om extern resurs kan komma i kontakt med säkerhetsskyddsklassad information.

Medarbetare ska vid osäkerhet av identitet kräva legitimation av servicepersonal som kommer till platsen för åtgärdande av fel. Vid behov ska även kontroll ske hos systemadministratören att service är beställd och att personalen är behörig.

11. Styrning av nätverk

11.1. Säkerhet vid datakommunikation

Lämpligt skydd ska finnas för att åstadkomma säkerhet för data i nätverk och för att skydda anslutna tjänster mot obehörig åtkomst. För att skydda sekretess och riktighet när data passerar allmänna nät och för att skydda anslutna system ska särskilda åtgärder vidtas.

Åtgärder för att förhindra eller minska risker inkluderar

- begränsning av åtkomstmöjligheter till det lokala nätverket,

- skydd av överförd information,

- rutiner för avbrottshantering och

- fysiskt skydd av kommunikationsutrustning.

Vid externa anslutningar ska varje kontaktyta utåt utredas med avseende på IT-säkerheten. Det ska finnas aktuell förteckning över samtliga externa anslutningar.

11.2. Uppringda förbindelser

Antalet uppringda förbindelser till det lokala nätverket ska minimeras.

Uppringbara förbindelser ska vara försedda med funktionerna identifiering, lösenord och pinkod eller säkerhetskort. Endast programvara anvisad av IT-enheten får användas.

Målsättningen ska vara att styra all extern kommunikation till kommunkoncernens IT-system via Internet.

11.3. Fasta förbindelser

Vid fasta uppkopplingar ska brygga/router med filterfunktion användas.

11.4. Internet

Varje användare måste beakta att Internet är ett allmänt öppet nät utan i förväg inbyggda säkerhetsfunktioner.

Viruskontroller ska köras kontinuerligt i nätverket och på arbetsstationer. Samtliga postsystem ska ha inbyggd viruskontrollfunktion för ingående och utgående post.

Publika web-servrar ska vara separerade från de interna näten.

12. Telefonväxel

Samma förutsättningar gäller för telesystemen som för övriga datasystem. Frågor angående integration mellan telefoni och datasystem ska ske i samråd med IT-enheten.

Endast servicepersonal ska ha tillträde till lokaler för televäxelutrustning. Telefonlösningar som bygger på funktionsavtal ska SUA-upphandlas.

Telefonnummer som ska spärras beslutas av kommundirektören efter samråd med IT-enhetens chef. Beslut om spärrning av telefonnummer återrapporteras till kommunstyrelsen.

13. Styrning av åtkomst

Verksamhetskrav och säkerhetskrav ska styra åtkomst till information och kommunkoncernens processer.

13.1. Regler och rutiner för behörighetsadministration

Regler och rutiner ska täcka alla stadier i användaråtkomsten, från registrering av ny användare till slutlig avregistrering.

Systemansvarig tilldelar och följer upp rättigheter i verksamhetssystemen och introducerar varje ny användare innan åtkomst tilldelas. Nätverksresurser tilldelas av IT-enheten i samråd med respektive systemansvarig. Beställning, ändring och avbeställning av behörighet görs av närmaste chef. (Förslag till blankett se bilaga 2.)

Varje användare ska ha en unik användaridentitet. Den tilldelade åtkomstnivån ska vara anpassad användarens arbetsuppgifter. Åtkomsträtten ska omedelbart tas bort när personer byter arbetsuppgifter eller lämnar kommunkoncernen.

Samtliga användare ska tillämpa följande riktlinjer för hantering av lösenord

- hemlighålla lösenorden,

- ändra lösenord regelbundet

- välja lösenord med minst sex tecken, bokstäver (inte å ä ö) och siffror,

- undvika att dokumentera lösenord på papper om inte detta kan förvaras helt säkert,

- ändra lösenord genast om lösenordssäkerheten äventyras,

- undvik lösenord som lätt kan härledas till omgivningen eller till den egna personen,

- ändra tillfälliga lösenord vid första inloggningen.

Användare som lämnar sin IT-utrustning utan tillsyn ska låsa arbetsstationen eller aktivera lösenordsskyddad skärmsläckare, alternativt logga ut ur nätverket. Varje användare ska logga ut ur nätverket efter arbetsdagens slut.

13.2. Styrning av åtkomst till nätverk

Åtkomst till både interna och externa nätverk ska styras för att trygga säkerheten.

För att arbeta mellan olika nätverk - fysiska, logiska och publika - krävs autentiserings- och krypteringsrutiner. Rutinerna meddelas av IT-enheten.

13.3. Övervakning av systemåtkomst och systemanvändning

Där det finns författningskrav på loggning skall systemet ha inbyggd loggningsfunktion.

Riskanalys ska ligga till grund för att bestämma nivå på övervakning och loggning av system.

13.4. Mobil datoranvändning och distansarbete

Distansarbete ska vara godkänt av verksamhetschef eller bolagsdirektör.

När mobil och bärbar datorutrustning inklusive mobiltelefoner och handdatorer används, ska särskild försiktighet iakttas för att säkerställa att inte verksamhetsinformation äventyras. Samma krav gäller på fysiskt skydd, styrning av åtkomst, krypteringsteknik, säkerhetskopiering och virusskydd som för stationär datorutrustning.

Utbildning ska ges till personal som använder mobila datorer och utrustning för distansarbete. Utbildningen ska innehålla information om riskerna med distansarbete och vilka säkerhetsåtgärder som behövs.

14. Systemutveckling

Nya lösningar ska i första hand sökas bland den allmänna marknadens produkter eller tjänster. I andra hand ska möjligheterna att anpassa produkter eller tjänster som finns på marknaden prövas. I tredje hand prövas nyutveckling för de specifika behoven. Samråd ska då ske med IT-arbetsgruppen.

Utveckling och underhåll av egenutvecklade system behandlar vi inte vidare i detta dokument.

15. Kontinuitetsplanering för verksamheten

Varje verksamhet ska upprätta en kontinuitetsplan. Syftet är att minska skada som förorsakas av säkerhetsincidenter och katastrofer genom en kombination av förebyggande och återställande skydd.

Följderna av eventuella katastrofer, incidenter och förlust av verksamhetsstöd ska analyseras. Avbrottsplan ska upprättas och införas för att säkerställa att funktioner kan återställas inom acceptabel tid. Planerna ska hållas uppdaterade och testas så att de blir ett integrerat inslag i alla ledningsrutiner. Planerna ska hanteras som känslig information.

Kontinuitetsplaneringen ska inledas med att identifiera de händelser som kan orsaka störningar i verksamheten. För att bedöma följderna av sådana störningar ska en riskanalys genomföras. Beroende av resultatet av riskanalysen ska en strategi utvecklas för att bestämma hur kontinuitetsfrågorna ska hanteras. Strategin ska fastställas av nämnd/styrelse.

Verksamheterna ska säkerställa att kontinuitetsplanerna är konsekventa och ange rutiner för underhåll. Varje verksamhet ska även klart ange villkoren för att aktivera planen liksom de personer som ansvarar för genomförandet av varje steg i planen.

16. Efterlevnad

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 sker av att säkerhetsrutinerna utförs och att 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.

Bilaga 1

Riktlinjer för hantering och skydd av sekretessbelagd och känslig information

Sekretessbelagd information får endast vara tillgänglig för den som behöver den för att fullgöra sina arbetsuppgifter eller för den som har lagligt stöd att få tillgång till informationen. Den som skapar information är ansvarig för att den blir hanterad på rätt sätt och för att känslig och sekretessbelagd information inte lämnas ut till obehörig.

- Handlingar ska förvaras och arkiveras i låst dokumentskåp eller säkerhetsskåp.
- Elektronisk information ska lagras på anvisad server eller krypterad hårddisk.
- Handlingar får inte ligga kvar på skrivbordet när rummet lämnas.
- Handlingar får inte förvaras utanför kontoret utan godkännande av verksamhetschef och bolagsdirektör.
- Om handlingar förvaras utanför kontoret ska de låsas in i säkert utrymme.
- Under resor ska handlingar medföras som handbagage eller i låst väska.
- Sekretessbelagd information ska förstöras i godkänd dokumentförstörare.
- Information lagrad på hårddisk, diskett, cd eller annan datamedia ska förstöras mekaniskt.
- Handlingar som skickas med internpost ska läggas i igenklistrat kuvert märkt med mottagarens namn. Posten får endast öppnas av adressaten. Vid frånvaro (t.ex. semester eller sjukdom) bör rutiner finnas för att post inte ska bli liggande.
- Handlingar som skickas med extern post ska rekommenderas
- Sekretessbelagda handlingar får endast i undantagsfall skickas med fax. Mottagaren ska då meddelas i förväg för att kunna ta emot faxmeddelandet personligen
- Sekretessbelagd information får inte skickas med okrypterad e-post
- Samtal om sekretessbelagd information bör endast i undantagsfall föras via mobiltelefon

Bilaga 2

Förslag till blankett för beställning/ändring/avbeställning av behörighet

Kryssmarkera typ av beställning:
ny behörighet (**N**)
ändring av behörighet (**Ä**)
borttag av behörighet (**B**)

Verksamhetsövergripande system

Systemnamn	Systemägare/Systemansvar	N	Ä	B
Nätverket, Novell NetWare	Kommunstyrelsen/IT-enheten/Lars Andersson			
Mailsystem Group Wise,	Kommunstyrelsen/IT-enheten/Lars Andersson			
WinÄss	Kommunstyrelsen/			
Persona	Kommunstyrelsen/			
Devis-X	Kommunstyrelsen/Peter Nordberg			
Fir/Kid	Byggnadsnämnden/Yvonne Stranne			
Autokavy	Byggnadsnämnden/Yvonne Stranne			

Verksamhetsspecifika system

Systemnamn	Systemägare/Systemansvarig	N	Ä	B

Användaruppgifter

Namn:
Personnummer:
Verksamhet:
Datum då beställningen senast ska vara utförd:
Övrigt:

Ovanstående beställning godkännes

…….…… ..……

Underskrift (närmaste chef) *Datum*