

Kapitel 3 Säkerhetspolicy

Inledning

I appendix A till SS 62 77 99-2 refereras till normativa krav för att uppfylla ett ledningssystem för informations säkerhet. Nedan följer råd som finns i SS-ISO/IEC 17799 för att kunna uppfylla dessa krav. Det är viktigt att veta att inte alla råd finns i SS-ISO/IEC 17799 återfinns som krav i SS 62 77 99-2. Mål och styrmiddel införs i den mån verksamheten så kräver – de kan även vara tillägg som inte återfinns i SS-ISO/IEC 17799.

Mål: Att ge ledningens viljeinriktning och stöd för informationssäkerhet.

Organisationens ledning bör, genom att fastställa och underhålla en informationssäkerhetspolicy för hela sin organisation klart ange viljeinriktning och visa sitt stöd och åtagande för informationssäkerhet.

Informationssäkerhetspolicyen är ledningens instrument för att klart ange inriktningen och visa sitt engagemang för informationssäkerheten – "det här är vår avsikt, så här vill vi ha det och så når vi dit".

Att tillföra företagskulturen en ny dimension – "i vår verksamhet är säkerhet ett självklart inslag i arbetet". Den ger ökad trygghet, trivsel och bidrar till ett bättre resultat. Den ska också vara en plattform för konsekvent agerande, göra de anställda medvetna om säkerhetens betydelse samt visa vägen för att uppnå säkerhetsmålen.

Informationssäkerhetspolicyen ska besvara följande frågor:

- Vad är det som ska skyddas?
- På vilken nivå ska skyddet vara?
- Vem är ansvarig för informationssäkerheten?
- Hur bedrivs informationssäkerhetsarbetet?
- Var gäller informationssäkerhetspolicyen?
- Hur ska informationssäkerhetspolicyen följa verksamheten och hotbilden?
- Vilka rättigheter och skyldigheter har medarbetarna?
- Hur ska incidenter hanteras?
- Påföljder då informationssäkerhetspolicyen ej följs?

Utan en informationssäkerhetspolicy är risken stor att frågor uppstår som kan skada verksamheten på olika sätt:

- Vad är det som gäller? Oklarheter i organisationen.
- Vem är ansvarig för vad? Varför ska jag göra något när ingen annan gör det?
- Vad anser ledningen egentligen? Allt är ju prioriterat!
- Det är svårt att skapa underliggande dokument som riktlinjer, anvisningar och instruktioner.
- Vi får inte mellanchefer att prioritera säkerhetsarbetet.

Det finns tillfällen då informationssäkerhetspolicyen har ett extra stort värde. Det kan röra sig om verksamheter som har speciellt skyddsvärd information som personuppgifter och finansiell verksamhet. Det kan också vara att säkerheten precis blivit en viktig fråga och det finns ett behov av att markera vad som gäller. Ytterligare ett exempel kan vara att man går in i ett nytt verksamhetsområde.

3.1 Informationssäkerhetspolicy

Organisationer som har ett markant säkerhetsinslag i sin verksamhet – nationella som internationella, privata som statliga – har en av ledningen uttalad och antagen informationssäkerhetspolicy som

- kan delges interna och externa intressenter vilket minskar risken för missförstånd och kan öka affärsmöjligheter och minska affärsrisken/-riskerna,
- underlättar granskning av det verkliga tillståndet med hänsyn till informationssäkerhetspolicyen.

En informationssäkerhetspolicy ska peka ut den övergripande inriktningen, slå fast de principer som ska gälla och tydliggöra organisationens inställning till arbetet, i detta fall informationssäkerhetsarbetet.

För att en informationssäkerhetspolicy ska få avsedd effekt är det några punkter som bör beaktas vid framtagandet av informationssäkerhetspolicyen. Den ska

- vara relevant i förhållande till organisationens verksamhet,
- vara långsiktig,
- vara övergripande,
- visa ambitionsnivå och inriktning,
- vara kommunicerbar med organisationens samarbetspartners,
- ha ett enkelt språk,
- vara kortfattad,
- föras ut på ett tydligt sätt.

En informationssäkerhetspolicy är ett centralt och viktigt dokument som utgör grunden för organisationens övergripande och detaljerade säkerhetsmål.

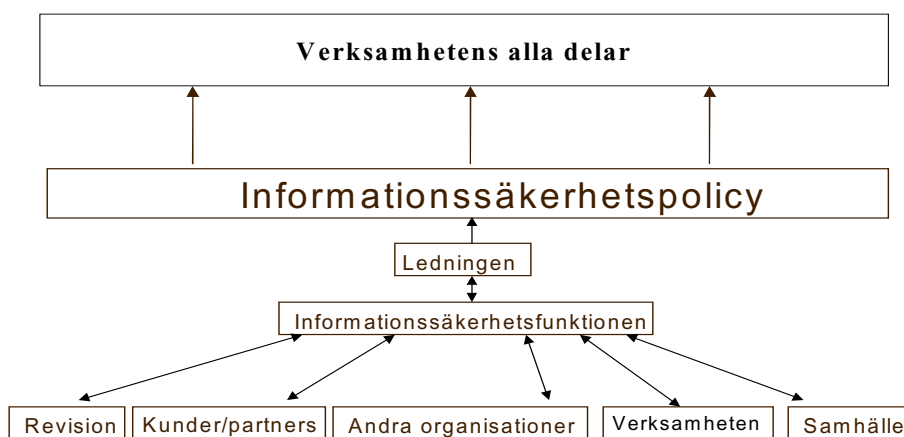
Det är organisationens högsta ledning som fastställer informationssäkerhetspolicyen och därmed också ansvarar för dess innehåll och att den uppfylls. Ansvar, befogenheter, arbetssätt och beslutsordning i speciella frågor liksom verksamhetsinriktning på kort sikt (1–3 år) kan vidareutvecklas inom organisationen och beslut ska framgå av ett upprättat protokoll.

Organisationen måste kunna redovisa och dokumentera på vilket sätt man följer upp sina åtagande enligt informationssäkerhetspolicyen. Det ska därför med hjälp av fastlagda rutiner dokumenteras och säkerställas vilka resultat som uppnåtts för att leva upp till innehållet i och innebörden av informationssäkerhetspolicyen.

Såväl leverantörer och entreprenörer som kunder och samarbetspartners ska informeras om organisationens informationssäkerhetspolicy och syn på säkerhet samt de önskemål och krav som är förknippade med detta. Det innebär exempelvis att organisationens entreprenörer måste leva upp och ta hänsyn till organisationens informationssäkerhetspolicy.

3.1.1 Att ta fram en informationssäkerhetspolicy

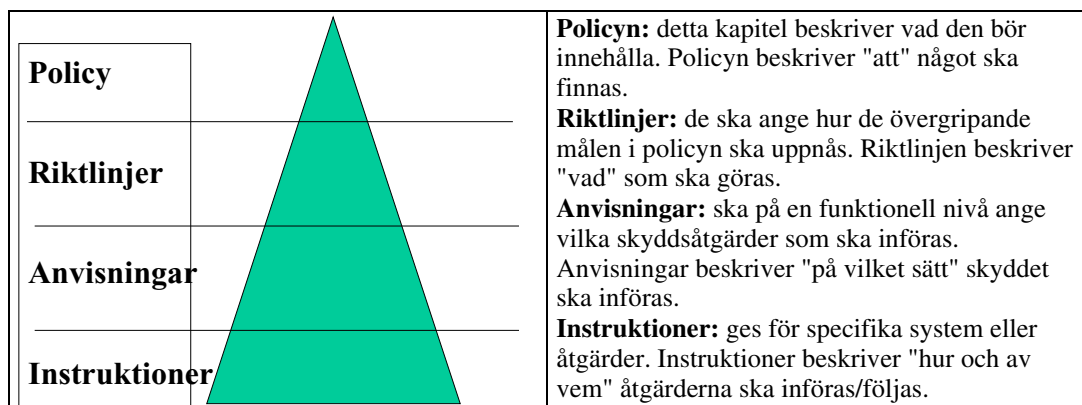
Informationssäkerhetspolicyen måste växa fram stegvis och vara förankrad i verksamheten. Den ska vara godkänd av ledningen. Efter beslut ska informationssäkerhetspolicyen förankras i verksamhetens alla delar.



En informationssäkerhetspolicy kan tas fram enligt följande steg:

1. Gå igenom frågelistan (se punkt 3.2 Underlag för att skriva en informationssäkerhetspolicy) och skaffa svar på frågorna. Välj struktur och mall (se punkt 3.3 Exempel på informationssäkerhetspolicy) för hur informationssäkerhetspolicyen ska utformas.
2. Ta ställning till de svar du fått på frågorna.
3. Stäm av relevansen i informationssäkerhetspolicyen genom att intervjua nyckelpersoner i verksamheten.
4. Förankra informationssäkerhetspolicyen i verksamheten.
5. Fastställ informationssäkerhetspolicyen i ledningen.
6. Inför och förankra den i organisationen.
7. Vid behov, minst årligen, revidera informationssäkerhetspolicyen.

Parallellt med arbetet att ta fram informationssäkerhetspolicyen bör en plan hur den ska förankras i verksamheten tas fram. I större organisationer kan det vara bra med en mix av åtgärder som exempelvis en kortfattad folder, presentationer ute i verksamheten, via intranet eller informationssäkerhetspolicyen som en bilaga i lönebeskedet. En informationssäkerhetspolicy antagen av ledningen visar ledningens viljeinriktning och utgör en vägledning för den fortsatta utvecklingen av informationssäkerhetsarbetet och hur det ska bedrivas. En del i detta arbete är att ta fram det underliggande regelverket baserat på organisationens processer.



Exempel på områden att beakta vid utformning av policy, riktlinjer, anvisningar och instruktioner:

- Säkerhetsansvar och säkerhetsorganisation.
- Säkerhetsplan.
- Incidenthantering.
- Risk- och sårbarhetsanalys.
- Lagar och bestämmelser.
- Informationsklassning.
- Hantering av information.
- Datariktighetsskydd.
- Tillgänglighetsskydd.
- Spårbarhet.
- Logiskt åtkomstskydd.
- Fysisk säkerhet.
- Personal.
- Nyckelpersoner.
- Externa resurser/användare.
- Information och utbildning.
- Persondatorer och arbetsstationer.
- Nätverk, tele- och datakommunikation.
- E-post och Internet.
- Systemutveckling/miljö.
- IT-drift.
- Systemförvaltning.
- Ändringshantering.
- Kontinuitetsplanering

Omfattningen kan begränsas med hänsyn till organisationens storlek.

3.1.2 Nyckelpunkter i informationssäkerhetspolicyn

Informationssäkerhetspolicyn bör ses som ett komplement till organisationens affärsplan, IT-strategi och de lagar och avtal som finns. Nedan följer ett antal nyckelpunkter som bör ingå:

- Viljedeklaration från högsta ledningen.
- Fastläggande av att säkerheten är viktig i verksamheten där informationssäkerhetens betydelse för verksamheten anges.
- Definition av begreppet "informationssäkerhet".
- Definiera vilken säkerhet som behövs i organisationen utifrån:
 - hot-, sannolikhets- och konsekvensbeskrivning,
 - omvärldens krav och/eller förväntningar (lagar, avtal och andra krav),
 - den personliga säkerheten,
 - incidenthantering.
- Visa på vilket sätt säkerhet lönar sig.
- Övergripande mål och detaljmål för säkerhetsarbetet.
- Beskrivning av kopplingen till andra styrande dokument eller rutiner.
- Ansvarsfördelning inom organisationen med en betoning på det personliga ansvaret.
- Beskrivning av säkerhetsorganisationens utseende, befattningsinnehavare och ansvar.
- Redogörelse för vikten av en kontinuitetsplan för verksamheten.
- Plan för informationssäkerhetspolicyns förverkligande genom exempelvis
 - information/utbildning,
 - säkerhetshöjande åtgärder.
- Beskrivning av uppföljningssystem.
- Påföljder vid åsidosättande av informationssäkerhetspolicyn eller andra säkerhetsregler.
- Angivande av dokumentansvarig för informationssäkerhetspolicyn och hur den ska revideras och följas upp.

Checklista – Informationssäkerhetspolicy

Fråga	Ja	Delvis	Nej
Ger informationssäkerhetspolicyn ledningens viljeinriktning och stöd för informationssäkerhetsarbetet?			
Har ledningen fastställt informationssäkerhetspolicyn?			
Är det beskrivet hur informationssäkerhetspolicyn ska underhållas och på vilket sätt?			
Är informationssäkerhetspolicyn förankrad i verksamheten och finns det ett system för detta?			
Finns det en definition av informationssäkerhetsbegreppet?			
Tar informationssäkerhetspolicyn hänsyn till hoten från anställda och utomstående?			
Visar informationssäkerhetspolicyn mål och omfattning samt vikten av informationssäkerhet?			
Är ansvaret definierat?			
Finns det reglerat hur rapportering av incidenter ska gå till?			
Hänvisar informationssäkerhetspolicyn till andra styrande dokument inom organisationen?			
Är det klart och tydligt beskrivet vem som är ägare till informationssäkerhetspolicyn?			

3.2 Underlag för att skriva en informationssäkerhetspolicy

Det är viktigt att skaffa sig underlag innan man börjar skriva informationssäkerhetspolicyn. I texten nedan finns ett antal frågor som är viktiga att ställa sig innan man börjar skriva.

1. Vilket mål har organisationen för sin verksamhet?
2. Vad är prioriterat i verksamheten?
3. Vad säger IT-strategin?
4. Finns det något fastställt dokument som beskriver dokumentnivåer i verksamheten (policy, riktlinjer, anvisningar, instruktioner)?
5. Finns det någon allmän säkerhetspolicy för organisationen?
6. Vilken information ska omfattas av informationssäkerhetspolicyn?
7. Vilka problem ska lösas med informationssäkerhetspolicyn?
8. Vad ger analyserna för underlag till informationssäkerhetspolicyn (risk-, affärsberoende- och säkerhetsanalys)?
9. Kan avsteg från informationssäkerhetspolicyn tillåtas? Hur ska sådana avsteg regleras/hanteras?
10. Vilka påföljder kan vara aktuella om informationssäkerhetspolicyn inte följs?
11. Krav på riktlinjer för informationssäkerheten?
 - internet?
 - e-post?
 - personlig integritet?
 - användningssätt?
 - konfidentiell/sekretessbelagd information?
 - programvarulicenser?
 - utläggning (outsourcing)?
12. Finns det en revideringsperiod för informationssäkerhetspolicyn?
13. Vilka hot finns mot organisationen (i dag och i framtiden)?
14. Mot vilken typ av information riktas hoten?
15. Har sannolikheten för och konsekvensen av dessa hot analyserats?
16. Vilka resurser ska skyddas?
17. Sekretess/riktighet/tillgänglighet?
18. Fred-, kris- och krigsaspekten, påverkar detta hur informationssäkerhetspolicyn utformas?
19. Vilken är den önskade nivån för informationssäkerhet?
20. Skyddskrav på utrustning och information utanför arbetsplatsen?
21. Tredje parts tillgång till information?
22. Hur fördelas kostnaderna för informationssäkerhetsåtgärder?
23. Hur mycket har investerats i fysiska skyddsåtgärder?
24. Hur mycket kostar den personella bevakningen per år?
25. Är ledningen involverad i säkerhetsarbetet?
26. Vem hanterar säkerhetsfrågor i organisationen?
27. Vem har ansvaret för säkerhetsfrågor i organisationen?
28. Finns det en säkerhetschef eller motsvarande?
29. Beslutsnivåer för säkerhetsfrågor?
30. Känner cheferna till verksamhetens säkerhetsregler?
31. Finns det en samordningsgrupp för säkerhet?

32. Vilka instruktioner om informationsskydd finns i dag?
33. Finns det anvisningar om klassificering av information?
34. Hur sker kunskapsspridningen rörande säkerhetsfrågor?
35. Finns det någon intern utbildning i säkerhet?
36. Finns det behov av utbildning i säkerhet?
37. Är informationssäkerhet kopplad till det övriga arbetet/säkerhetsarbetet?
38. Vem ska ha tillgång till vilken information?
39. Åtkomsträttigheter?
40. Loggning?
41. Extern kommunikation?
42. Externa beroenden?
43. Förekommer distansarbete?
44. Får användare ta hem arbetsutrustning?
45. Incidenthantering?
46. Kritiska händelser de senaste 3 åren?
47. Hur ser skadestatistiken ut?
48. Hur bedriver organisationen det skadeförebyggande arbetet?
49. Finns rutiner för att hantera skador/incidenter?
50. Erfarenheter av skador/incidenter?
51. Förändringar som gjorts i system/rutiner efter en skada/incident?
52. Medverkandes ansvarsområden?
53. Hur stor är personalomsättningen?

3.3 Exempel på informationssäkerhetspolicy

3.3.1 Informationssäkerhetspolicy för Medytekk

Daterad 2003-xx-xx.

Fastställd av företagsledningen 2003-xx-xx.

All personal ska tilldelas ett personligt exemplar av informationssäkerhetspolicyn.

Informationssäkerhetspolicyn kommer att presenteras vid interna möten under hösten.

Motiv

Vi som arbetar på Medytekk använder IT för att stödja, utveckla och effektivisera verksamheten. Vårt företag är beroende av informationsbehandlingen. Kraven på snabb och relevant information inom olika funktioner av Medytekk:s verksamhet ökar. Att säkerställa hög tillgänglighet och samtidigt innehålla nödvändiga krav på sekretess är väsentligt ur affärssynpunkt.

Definition

Informationssäkerhet inbegriper all säkerhet kring Medytekk:s totala informationsbehandling. Såväl organisatoriska åtgärder som fysiska och logiska skyddsåtgärder inbegrips. Exempel på säkerhetsrelaterade åtgärder är en fastställd informationssäkerhetspolicy, ansvarsfördelning, utbildning, riskanalys, katastrofplan, behörighetsregler, informationsklassning, säkrad driftmiljö, åtkomstskydd i datorer, regler för hantering av datamedia, behörighetsadministration, säkerhetskopiering, regler för extern kommunikation och modemuppkopplingar etc och kontroll av uppgiven identitet vid till exempel påloggning med hjälp av aktiva kort (förstärkt autentisering).

För att tillgodose kraven som ställs på informationssystemen, där så gott som all Medytekk:s information hanteras på ett eller annat sätt, är det nödvändigt att hanteringen av information sker på ett så tillförlitligt sätt som möjligt.

Informationssäkerheten ska motverka risker för såväl obehörig läsning och förändring av data som för förlust av data. Informationssäkerheten syftar även på informationens kvalitet, riktighet och tillgänglighet.

Nyckelord för informationssäkerheten är att säkra informationens

- sekretess,
- tillgänglighet,
- riktighet,
- spårbarhet.

Informationssäkerhetspolicyn utgör ett komplement till Medytekk:s målbeskrivning och IT-strategi, som anger inriktningen för den totala informationsbehandlingen. Informationssäkerhetspolicyn är det grundläggande underlaget för informationssäkerhet och berör samtliga anställda, samarbetspartners och konsulter.

Informationssäkerhetspolicyn ger inriktningen och de övergripande målen för hur informationssäkerhetsarbetet ska bedrivas inom företaget - för verksamheten, personalen, kunderna och samarbetspartners.

Tillhörande dokument

Riktlinjer för informationssäkerhet är ett deldokument till informationssäkerhetspolicyn som beskriver riktlinjerna för informationssäkerhetsarbetet. Detta deldokument innehåller motiv, mål, tidplan, definition, omfattning och ansvarsfördelning.

Som ett komplement till den övergripande informationssäkerhetspolicyn och riktlinjerna kommer dokument att finnas i form av anvisningar inom olika områden för informationssäkerhetsarbetet. Dessa samlas i en informationssäkerhetshandbok som sammantaget visar hur informationssäkerhetsarbetet ska bedrivas. För specifika områden kan det även finnas instruktioner på en mer detaljerad nivå som beskriver vad som gäller. Dessa dokument beskriver tillsammans alla fysiska och logiska åtgärder som syftar till att förebygga eller minimera oönskade konsekvenser av olika händelser på informationssystemsområdet.

Mål för informationssäkerheten

Målsättningen med denna informationssäkerhetspolicy är att säkerställa sekretess, tillgänglighet och spårbarhet för verksamhetens information och data, samt att reducera risken för skador på verksamheten oavsett orsak och angripare.

- Avsikten med denna informationssäkerhetspolicy är att skydda organisationens informationstillgångar mot alla typer av hot - interna eller externa, avsiktliga eller oavsiktliga.
- Det ska finnas skyddsmekanismer som utifrån nedanstående punkter säkerställer informationens
 - sekretess,
 - tillgänglighet,
 - riktighet,
 - spårbarhet.
- Informationssäkerhetsarbetet ska bedrivas enligt standarden SS-ISO/IEC 17799.
- Alla anställda inom organisationen som i sina arbetsuppgifter berörs av it ska vara medvetna om informationssäkerhetsfrågornas betydelse samt ha kunskaper om vad som gäller för att bevara och utveckla en säker och stabil IT-miljö.
- Informationssäkerheten ska vara en integrerad del i Medytekkts ordinarie verksamhet och stödja verksamheterna i att uppnå de uppsatta målen för kvalitet och effektivitet.
- Till grund för informationssäkerhetsåtgärder ska föreliggande dokumenterade bedömningar eller genomförda riskanalyser.
- Skydden för kända hot ska vara uppbyggda till rätt nivå med hänsyn till skyddskostnad och konsekvens för Medytekkts verksamhet vid eventuellt tillfogad skada.
- Alla säkerhetsincidenter, konstaterade eller misstänkta, ska rapporteras till och utredas av informationssäkerhetschefen.
- Uppföljning av riskanalyser, skyddsåtgärder och utbildningsinsatser ska ske kontinuerligt.
- En kontinuerlig drift ska garanteras genom att säkerställa driftmiljön för samtliga datordriftställen.
- Medytekk ska ha egen IT-personal, det vill säga anställda med rätt kompetens och som fortlöpande utbildas i takt med att datorsystemen utökas och förändras.
- Känslig data ska skyddas mot otillbörlig åtkomst inom och utom företaget med hjälp av behörighetskontroll och i vissa fall kryptering.
- Säkerhetsarbetet ska skydda personalen i dess tjänsteutövning.
- Kommunikationslösningar ska vara gjorda så att resursdatorer och nätverk skyddas mot driftsstörningar och intrång. Driftsstörningar och intrång ska kunna följas upp med hjälp av dokumenterad historik (loggar).
- Man ska leva upp till gällande lagar och kommersiell sekretess. Exempelvis ska personuppgiftslagen (PUL) följas så att den personliga integriteten beaktas i användningen av personregister. Bokföringslagen ska följas vad gäller ansvarsfördelning och behandlingshistorik för att uppnå en tillförlitlighet och en god intern kontroll av redovisningen.

Omfattning

Informationssäkerhetspolicyn rör all informationsbearbetning oavsett driftmiljö, alltså oberoende av om datorbearbetningen sker i resursdator (stor-, minidator, eller server) eller persondator.

Informationssäkerhetspolicyn gäller även om datorbearbetningen sker externt och via datakommunikation eller motsvarande. Med datorbearbetning menas hela informationssystemet: system-/programutveckling, källdataframställning, registrering, dataöverföring, bearbetning, datalagring, utdatahantering, arkivering och makulering.

Genomförande

För att nå de uppsatta målen ska resurser avdelas för att systematiskt genomföra

- riskbedömningar och konsekvensanalyser,
- riktlinjer och handlingsplan,
- informationssäkerhetshöjande åtgärder,
- utbildning och information.

Årligen ska en plan för säkerhetsarbetet inom varje avdelning upprättas. Planen ska innehålla en beskrivning av säkerhetsläget samt de planerade åtgärderna som ska vidtas för att höja säkerhetsnivån. Planerna sammanställs till en handlingsplan och en budget för informationssäkerheten för hela Medytekk. Ledningen fattar beslut om planen, dess genomförande och budget.

Övergripande ansvar

Företagsledningen är ytterst ansvarig för mål och ramar för informationssäkerhetsarbetet och bär det yttersta ansvaret för skador som kan inträffa. Ledningen följer upp informationssäkerhetsläget genom att ta del av säkerhetsplanen.

Ansvarsfördelning

Informationssäkerhetschefen sammanställer avdelningarnas säkerhetsplaner och upprättar en säkerhetsplan för hela Medytekk samt svarar för initiering och uppföljning av informationssäkerhetsarbetet enligt planen.

Säkerhetspolicy

Informationssäkerhetssamordnaren är ansvarig för att informationssäkerhetsåtgärder genomförs enligt ledningens och informationssäkerhetschefens beslut. Samordnaren ska leda informationssäkerhetsarbetet inom respektive tilldelat ansvarsområde och är även registeransvarig för avdelningens personregister.

Den system-/driftansvarige har det operativa ansvaret för att beslutade åtgärder genomförs. Ansvaret kan gälla ett eller flera IT-system. Den ansvarige är skyldig att omgående meddela säkerhetsproblem och misstanke om eller redan inträffade incidenter till informationssäkerhetssamordnaren eller informationssäkerhetschefen.

Användaren ska verka för en god informationssäkerhet inom sitt område och följa de regler och riktlinjer som gäller inom Medytekk. Nivån på informationsskyddet inom företaget beror på hur varje enskild person hanterar verktygen för informationsbehandling såsom datorer, disketter, datakommunikation (e-post, fax etc).

Dotterbolag/partners

I enlighet med företagsägarnas enhälliga beslut vid fastställandet av denna informationssäkerhetspolicy år 2003, gäller samma informationssäkerhetspolicy för dotterbolag och partners.

Informationssäkerhetspolicyns giltighet

Planering av framtida informationsstrategier ska ske i samarbete med respektive företagsledning.

Informationssäkerhetschefen ska arbeta för att informationssäkerheten i samtliga bolag uppnår jämlika nivåer till det fjärde kvartalet 2004. Revidering av informationssäkerhetspolicyn samt riktlinjerna kommer att göras därefter för att i ny upplaga börja gälla fr.o.m. 2005.