RAM ONE AB Informationssäkerhetspolicy

RAM ONE AB (nedan ”Bolaget”) organisationsnummer 556629-1950, Box 1744, 111 87 Stockholm har upprättat denna policy för att informera sina kunder om hur Bolaget vidtar lämpliga tekniska och organisatoriska åtgärder för att uppnå kraven i Personuppgiftslag (1998:204) 31 §.

Bakgrund

Bolaget anser att god informationssäkerhet är en investering och en försäkring för verksamhetens fortlevnad. Genom att utgå från verksamhetens behov av skyddsnivå kan informationssäkerhetsarbetet ständigt förbättras.

Utgångspunkten för Bolagets informationssäkerhetsarbete är att verksamhetens behov av säkerhetsskydd för troliga och oönskade framtida händelser. Bolagets informationssäkerhet utgör på så sätt en del av Bolagets totala riskhantering.

Syfte

Syftet med informationssäkerhet är att skydda Bolagets informationstillgångar från alla typer av hot, såväl externa som interna. Informationssäkerhet är grundläggande för att hantera informationsrisker på ett strukturerat och konsistent sätt. Denna policy anger inriktning och övergripande mål för informationssäkerhetsarbetet på Bolaget.

Grundläggande för Bolagets hantering av informationssäkerheten är:

- *Sekretess* – att ingen obehörig får tillgång till Bolagets information;
- *Riktighet* – att våra kunder alltid får rätt information;
- *Tillgänglighet* – att våra kunder har tillgång till den information som är kopplad till sin affärsrelation med oss.

Riktlinjer - mål och metoder för styrning samt struktur för riskbedömning

Information, data och informationssystem i alla sina former utgör några av de mest värdefulla tillgångarna i Bolaget. Samtliga medarbetare har ett ansvar att skydda dessa mot alla former av hot, såväl interna som externa, såväl avsiktliga som oavsiktliga.

Samtliga verksamhetsansvariga har ett ansvar för informationssäkerheten inom sitt ansvarsområde. Riskanalyser ska genomföras årligen inom de affärskritiska processerna. Dessa ska genomföras med den metod och de mallar som har framtagits för detta ändamål.

Resultatet av de genomförda riskanalyserna på aggregerad nivå ska presenteras för ledning och styrelse. Denna rapportering genomförs årligen under våren av CAG Datastöd AB.

Bolaget ska efterleva gällande lagstiftning. Säkerheten ska vara en integrerad del av Bolagets verksamhet och stödja verksamheten i att uppnå de uppsatta målen för kvalitet och effektivitet.

Organisation av informationssäkerheten

Inom Bolaget har informationssäkerhetsarbetet indelats i säkerhetsområden. Dessa omfattar fysisk säkerhet, administrativ säkerhet, datasäkerhet/IT-säkerhet, personsäkerhet samt kommunikationssäkerhet.

Med *fysisk säkerhet* menas skydd av lokaler och medarbetare genom larm, brandvarnare och genom utbildning av samtliga medarbetare i säkerhetsfrågor.

Med *administrativ säkerhet* menas det övergripande informationssäkerhetsarbetet genom policy, kontinuitetsplaner, incidentdatabas, övergripande anvisningar och regelverk.

Med *datasäkerhet/IT-säkerhet* menas skydd av de servrar och lagringsmedia där all information lagras samt skydd av data och kommunikation genom e-post, på Bolagets intranät med mera.

Med *kommunikationssäkerhet* menas skydd av de medier som används för att kommunicera med omvärlden, exempelvis fax, telefoni och e-post.

Rapportering och uppföljning

Ledning och styrelse har det övergripande ansvaret för informationssäkerhetsarbetet. Administrativ chef har fått ledningens ansvar att vidta nödvändiga åtgärder så att säkerhetsarbetet har en acceptabel nivå med hänsyn till kostnaderna för att implementera dessa och de konsekvenser som en inträffad incident kan orsaka Bolaget. När det gäller datasäkerhet/IT-säkerhet ligger ansvaret på internt IT-ansvarig.

Uppföljning av informationssäkerhetsarbetet sker genom att samtliga säkerhetsincidenter registreras och kostnadssätts i avsett system. Uppföljning av skyddsåtgärder, gjorda med utgångspunkt från genomförda riskanalyser, ska ske kontinuerligt.

Kontinuitetsplanen antas årligen av ledningen. Den reglerar och definierar de kritiska verksamhetsprocesser som ska fungera vid allvarliga incidenter.

Ledningen ska årligen följa upp genomförda riskanalyser. Rapportering görs av Intern IT- ansvarig till ledningen.

Tillhörande dokument

Till stöd för informationssäkerhetsarbetet finns rutiner för hantering av säkerhetssystem, klassificeringsäkerhetsregler för säker arbetsplats och inpasseringsrutiner.

Ansvar

Policyn fastställs av Bolagets styrelse årligen. Adminstrativ chef ansvarar för att säkerhetspolicyn och tillhörande dokument uppdateras och sedan kommuniceras till samtliga medarbetare.

Samtliga medarbetare har ett ansvar att följa Bolagets säkerhetsregelverk.

Avsiktliga eller oavsiktliga avsteg från denna policy kommer att utredas. En sådan utredning kan medföra att användarnas privata information kan komma att omfattas av en utredning om detta krävs av lagstiftning eller av andra myndigheter.