

INFORMATIONSSÄKERHETSPOLICY

Denna dag, 20210501, har följande policy upprättats för Linguacom.

Bakgrund

God informationssäkerhet är en investering och en billig försäkring för alla företag, oavsett storlek och verksamhet. Genom att utgå från verksamhetens behov av skyddsnivå kan informationssäkerhetsarbetet ständigt förbättras.

Utgångspunkten för allt informationssäkerhetsarbete ska vara verksamhetens behov av säkerhetsskydd för troliga och oönskade framtida händelser. Informationssäkerhet utgör på så sätt en del av företagets totala riskhantering och är en framgångsfaktor för varje företag.

Syfte

Syftet med informationssäkerhet är att skydda företagets 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 företaget.

Grundläggande för företagets hantering av informationssäkerheten är:

- Sekretess - att ingen obehörig får tillgång till företagets 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 de mest värdefulla tillgångarna i företaget. 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 informationssäkerhetschefen.

Säkerhetsarbetet ska bedrivas i enlighet med de internationella riktlinjerna för styrning av informationssäkerhet. Företaget ska efterleva gällande lagstiftning. Säkerheten ska vara en integrerad del av företagets verksamhet och stödja verksamheten i att uppnå de uppsatta målen för kvalitet och effektivitet.

Organisation av informationssäkerheten

Inom företaget 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 samt kommunikation genom e-post och på företagets intranät med mera.

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

Med personsäkerhet menas skydd av ledning och medarbetare från alla typer av incidenter och angrepp som kan ske genom rån, hot eller inträffade incidenter genom brand.

Rapportering och uppföljning

Ledning har det övergripande ansvaret för informationssäkerhetsarbetet. Vd eller den dom denne utser har av ledningen fått ansvar för 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 företaget.

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 informationssäkerhetschefen till ledningen.

Ansvar

Polycyn fastställs av företagets ledningsgrupp. Vd eller den dom denne utser ansvarar för att säkerhetspolycyn och tillhörande dokument uppdateras och sedan kommuniceras till samtliga medarbetare.

Vd eller den dom denne utser övervakar även policyns efterlevnad och att samtliga medarbetare får lämplig utbildning så att en ökad medvetenhet om informationssäkerhetsfrågornas relevans etableras i vårt företag. Samtliga medarbetare har ett ansvar att följa företagets 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.