IT- och säkerhetspolicy

Syfte

Syftet med denna policy är att säkerställa att arbetet med IT, säkerhet och informationssäkerhet utförs så att allvarliga säkerhetsincidenter eller kriser kan förebyggas och hanteras. Målet är att skydda företagets, kunders och andra intressenters information för att undvika allvarliga säkerhetsincidenter och kriser.

Målgrupp

Denna policy gäller för hela koncernen, såväl anställda som inhyrd personal. Var och en är ansvarig att följa denna policy samt tillhörande regelverk och rutiner och att dessa tillämpas inom det egna ansvars- och arbetsområdet.
Alla ska vara medvetna om vilket ansvar de har när det gäller informationssäkerhet genom tydliga riktlinjer för detta samt se sin funktion i säkerhetsarbetet och incidentrapportering som en naturlig del i vardagen.

Tillämpning

Den verkställande direktören är ytterst ansvarig för säkerhet och beredskap och ska tillse att ansvar och befogenheter förs ut i bolaget på sådant sätt att arbetet kan bedrivas verkningsfullt. För att denna policy ska anses efterlevd ska följande kriterier vara uppfyllda:

- Policyn ska vara kommunicerad och finnas lättillgänglig för alla medarbetare
- Policyn ska revideras årligen och uppdateras vid behov.

Riktlinjer

Säkerhet och trygghet, fysisk och teknisk säkerhet, kris- och incidenthantering samt informationssäkerhet ska bidra till att de långsiktiga strategiska affärsmålen kan uppnås genom förebyggande säkerhetsåtgärder och genom att identifiera och begränsa risker inom bland annat säkerhetsskydd, personskydd och förlust av materiella samt immateriella tillgångar till en acceptabel nivå. Säkerhetsarbetet ska vara ett stöd som gör att rutiner och arbetsmetoder i verksamheten både ger en hög säkerhet och en rationell verksamhet.

IT- och säkerhetspolicyn tillgodoser PEs:

- Säkerhet (att vara en säker samarbetspartner)
- Trygghet (trygg miljö för både medarbetare och besökare)
- Värna om materiella och immateriella värden
- Säkerhetsskydd
- Informationssäkerhet.

Säkerhet, sekretess och trygghet

PE ska verka för en säker och trygg arbetsplats genom att:

- Medarbetare ska ges information och efter behov utbildning om hot, risker och säkerhetsrutiner och särskild vikt ska läggas på skyddet av sekretessbelagd eller säkerhetsskyddsklassad information
- Skyddet för medarbetare som arbetar i sekretessklassade eller säkerhetsskyddsklassade uppdrag ska bedömas särskilt och få erforderlig säkerhets- och säkerhetsskyddsutbildning
- Säkerhetsrelaterade händelser och incidenter ska dokumenteras och rapporteras till säkerhetschefen
- PEs kontor ska skyddas mot otillbörlig åtkomst genom besökshantering och fysiskt skydd
- PE skall genom avtal säkerställa att leverantörer upprätthåller rätt säkerhetsnivå
- I avtal med underkonsulter eller leverantörer ska tydlig ansvarsfördelning och lämpliga säkerhetsåtgärder ingå och uppföljning möjliggöras
- Övergripande riskanalys för säkerhet och säkerhetsskydd ska utföras regelbundet, där brister följs upp genom etablering av handlingsplaner för att åtgärda bristerna
- Riskanalyser ska vara en naturlig del i planering eller vid förändring av verksamheter, lokaler, IT-system och rutiner
- Riskkostnaderna optimeras genom analys av skade-, försäkrings-, och skyddskostnader
- Utformningen av de vardagliga säkerhetskraven och säkerhetsrutinerna samt av katastrofplaner ska göras så att organisationen vid en krissituation i största möjliga utsträckning kan bibehålla ordinarie ledningsstrukturer, arbetssätt och rutiner

Säkerhetsskydd
PE är ansvariga för att hantera säkerhetsskydd i uppdrag genom att:

- Förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs
- Förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet
- Förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs
- Förebygga att personer som inte är pålitliga ur säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig
- Säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd.

Informationssäkerhet
PE strävar efter att säkerställa god tillgänglighet, konfidentialitet och integritet oavsett vilket media som informationen finns på.

Informationssäkerhet tillgodoser informationens:

- Sekretess (vem som har tillgång till informationen)
- Tillgänglighet (att informationen är tillgänglig för behörig)
- Riktighet (att informationen är tillförlitlig)

Vår verksamhet, anställda och kunder ska skyddas genom att lämpliga åtgärder kring informationssäkerhet vidtas. Åtgärderna baseras på vedertagen god praxis, identifierade risker, intressenters förväntningar, regelverk och tillämplig lagstiftning. Målet är att rätt information ska finnas tillgänglig för rätt person när den behövs.

Det innebär att vi identifierar i vilka processer, system, tjänster och produkter som persondata och affärskritiska data hanteras samt klassificerar och värderar denna för att kunna säkerställa adekvat skydd. Vi säkerställer också att det finns en incidenthanteringsprocess för hantering av informationssäkerhetsincidenter samt rapportering av dessa om behov föreligger.

IT-säkerhet
IT-säkerhet ingår som en bärande del i arbetet med informationssäkerhet och ska säkerställa att IT-system och IT-arkitektur skyddas med lämpliga säkerhetsåtgärder. Säkerhetsnivån baseras enligt god praxis på behovet av skydd för den information som överförs, bearbetas och lagras i våra IT-system och infrastruktur. IT-säkerheten ska utvärderas i samband med anskaffning, utveckling och förvaltning av IT-system och IT-infrastruktur oavsett om de hanteras i egen regi eller köps in som tjänster.

Intergritet och hantering av personuppgifter
Vi arbetar aktivt med att skydda personuppgifter för att skydda medarbetare, varumärke och förtroende på marknaden. Vi skall skydda information som rör personlig integritet med särskilt fokus på känsliga personuppgifter som kan uppfattas som kränkande, exempelvis uppgifter om hälsa eller facklig tillhörighet, något som medför risk för skadeståndskrav och sanktioner.

Säkerhetsåtgärder

Det finns system, rutiner och regler till stöd för denna policy.

Dessa omfattar:

- säkerhetsorganisation
- säkerhetsskyddsorganisation
- uppdrag med säkerhetsskydd
- tillträde till lokaler
- fysiskt skydd och teknisk bevakning i PE lokaler
- personsäkerhet
- informationssäkerhet
- säkerhetskopiering och redundans
- skydd mot skadlig kod
- lösenordshantering
- riskhantering
- incident- och krisberedskap
- kontinuitetsplanering

Ansvar och ständiga förbättringar

Vi arbetar aktivt för att säkerställa efterlevnad av lagar och regelverk i syfte att skydda kunder, medarbetare och andra intressenter. Vi tar ansvar för, och ser värdet av att arbeta långsiktigt. Vi har alla en strävan efter att ständigt förbättras och hela verksamheten bidrar till att vi når våra mål och uppfyller våra egna, våra kunders och ägares krav avseende IT och säkerhet.