Policy för Informationssäkerhet

1. Bakgrund

Wenells informationssäkerhetsarbete ska bedrivas på ett systematiskt, formaliserat och riskorienterat sätt och ta sin utgångspunkt i aktuell version av den internationella ledningssystemstandarden för informationssäkerhet, ISO/IEC 27001.

2. Syfte

Syftet och målsättningen med Wenells informationssäkerhetsarbete är att säkerställa ett väl avvägt skydd för Wenells informationstillgångar så att rätt information är tillgänglig för rätt person vid rätt tidpunkt och på ett spårbart sätt.

2. Policy

Ledningssystemet för informationssäkerhet (LIS) och tillhörande dokumentation omfattar Wenell alla informationstillgångar utan undantag, oavsett om den behandlas manuellt eller automatiskt samt Wenells medarbetare, anställda, konsulter och praktikanter.

Alla informationstillgångar och tillhörande IT-system, plattformar och produkter ska vara klassificerade med avseende på känslighetsgrad. Informationssäkerhetsarbetet ska ta sin utgångspunkt i regelbundna riskanalyser som syftar till att avväga rätt skyddsnivå i alla delar av Wenell, samt motivera investeringar eller utbildningsinsatser för att:

- förhindra eller försvåra för obehöriga att få tillgång till information (konfidentialitet)
- säkerställa att den information som produceras och bearbetas är korrekt, aktuell och fullständig (riktighet)
- bidra till att informationen är åtkomlig vid behov (tillgänglighet)
- säkerställa ursprunget av varje transaktion (spårbarhet)

För vart och ett av dessa områden ska organisatoriska, administrativa och tekniska skyddsåtgärder vidtas och dokumenteras på ett sådant sätt att det går att kontrollera att ett väl avvägt skydd uppnåtts.

Informationssäkerhetsskyddet ska granskas regelbundet för att utifrån tekniska ändringar och förändrade affärsprocesser säkerställa efterlevnaden av gällande lagar och LIS. Avvikelser, risker och incidenter ska systematiskt dokumenteras och följas upp, så att erfarenheter från dessa kan tas till vara som en del av det kontinuerliga förbättringsarbetet. Resultatet av informationssäkerhetsarbetet ska årligen redovisas vid ledningens genomgång.

3. Ansvar

Wenells styrelse beslutar om policyn, VD är ytterst ansvarig och det operativa genomförandet är delegerat till IT-ansvarig.

Wenells VD är ytterst ansvarig för informationssäkerheten och för övergripande säkerhetsfrågor av styrande karaktär. Ansvaret omfattar även att säkerställa att det finns ekonomiska och personella resurser med rätt kompetens för informationssäkerhetsarbetet.

Varje medarbetare, anställd, konsult och praktikanter som hanterar informationstillgångar i någon form har eget ansvar i sina roller att upprätthålla informationssäkerheten och förbinder sig att följa policyer och riktlinjer med tillhörande processer och anvisningar som finns beslutade.

Stockholm den 3 september 2024

……..

Tommy Olin, VD