



Informationssäkerhetspolicy

Allmänt

ID06 behandlar och lagrar en stor mängd data åt både företag och individer. Denna information har ett värde, dels för den enskilde dels för andra intressenter. Informationen behöver klassificeras, hanteras korrekt men också skyddas och göras tillgänglig för både personer och system när det så väl behövs. Allt detta samtidigt som lagar, förordningar och branschkrav ska efterlevas samt att våra intressenters förväntningar och krav på oss som företag uppfylls.

Omfattning

Data som vi hanterar i vårt ID06-system behöver leva upp till våra intressenters krav om en hög tillgänglighet och en hög tillförlitlighet parallellt som strategier och teknikval är framtidssäkrade, långsiktiga och stödjer våra kunders behov av konfidentialitet. Vi ska sträva mot en stimulering av digitalisering, finna nya användningsområden för våra intressenter under samma tid som vi minimerar sannolikheten för och konsekvenserna av att ett driftavbrott uppstår.

Flödet av olika typer av information inom ID06:s gränser ska vara identifierade och ses som våra primära tillgångar som behöver processas på säkra tekniska plattformar. Riskbedömningarna ska utföras kontinuerligt för att ge lämpliga analyser av lägesituationen och vilka säkerhetsåtgärder som behöver implementeras samt fastställa vilket behov det finns för både underhåll och utveckling av informationssäkerhetsskyddet.

För att konstruera ett ledningssystem och tillgodose att det fortlöpande förbättras ska alla ID06 AB:s medarbetare och, i förekommande fall, konsulter och leverantörer erhålla lämplig utbildning och fortbildning för ökad medvetenhet, samt regelbundna uppdateringar vad gäller organisationens policy, ID06 Standard och rutiner i den omfattning som är relevant för deras befattning och arbetsuppgifter.

Alla anställdas dagliga arbete ska genomsyras av följande punkter:

- Styrning. Processer, rutiner och instruktioner ska ligga till grund för allt arbete som berör information inom ID06 AB.
- Konfidentialitet. Det ska vara rätt skydd på informationen och systemen så att de inte avsiktligt eller oavsiktligt görs tillgängliga för obehöriga.
- Riktighet. Att information, system och tjänster ska ha den riktighet som intressenter förväntar sig. Det vill säga att informationen är korrekt, aktuell och begriplig för användaren.
- Tillgänglighet. Informationen ska vara tillgänglig för användaren när den behöver nå den.
- Spårbarhet. Det ska vara möjligt att spåra händelser till enskilda individer eller program vid en viss tidpunkt.

Alla medarbetare förväntas arbeta på ett sätt som är förenligt med informationssäkerhetspolicyen.