PROJKON

IT-säkerhetspolicy

Norrköping
Datum 2021-09-27
Ansvarig: Carl-Johan Bondesson

IT-SÄKERHETSPOLICY

Syfte

Syftet med IT-säkerhetspolicyn är att sätta riktlinjer för hur IT-säkerhetsarbetet inom Projkon ska bedrivas samt tydliggöra vilka värderingar företaget står för. IT-säkerhetsarbetet utgör inga separata aktiviteter som ligger utöver den ordinarie verksamheten utan är inordnat i allt arbete som Projkon utför.

IT-säkerhetspolicy

För att säkerställa en IT-miljö som är modern, säker och flexibel samarbetar Projkon med specialister i branschen som tillhandahåller dessa tjänster. I dagsläget Midpoint AB. Dessa skydd ska motstå externa såväl som interna hot. Följande principer avseende IT-säkerhet ska råda inom Projkon:

- Individens arbete ska kunna utföras med flexibel arbetsplats både på kontor och på annan valfri plats.
- IT-miljön ska innehålla ett modernt skydd för externa hot genom antivirusprogram och 2-faktorsinloggning.
- Datalagring ska utföras på gemensam databas med versionshantering för fullgott kontinuitetsskydd mot kryptovirus.
- Backupfunktioner ska finnas vid händelse av skada på enskild enhet eller på hela system.
- Inkommande mail ska granskas av säkerhetssystemet för skräppost och phishingförsök innan den övergår i användarens inkorg.
- Medarbetare rapporterar avvikelser avseende IT-säkerhet till Projkons IT-ansvarige.
- Säkerhetsarbetet ska innehålla periodiska kontroller av att funktioner som antivirusprogram är aktiva samt regelbundna förvaltningsmöten mellan tjänsteleverantören och Projkons IT-säkerhetsansvarige.
- Extern support används för att kunna ge svar på frågor avseende datorer, program inklusive säkerhetsfrågor

Ansvar

Ledningen inom Projkon ansvarar för att företagets medarbetare är förtrogna med företagets IT-säkerhetspolicy men det ligger på individens ansvar att följa den. Med det menas att policyn skall vara styrande i den dagliga verksamheten och i strategisk planering.