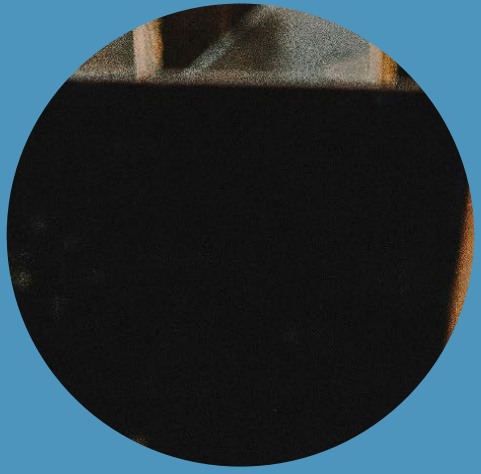
PUBLIC PEOPLE
Vi gör skillnad för offentlig sektor

# Informationssäkerhetspolicy

2024



PUBLIC PEOPLE
Vi gör skillnad för offentlig sektor

# Informationssäkerhetspolicy

Det övergripande syftet med Public Peoples informationssäkerhetsarbete är att säkerställa ett väl avvägt skydd för bolagets informationstillgångar så att rätt information är tillgänglig för rätt person vid rätt tidpunkt och på ett spårbart sätt.

Policyn gäller hela bolagets verksamhet, och arbetet med informationssäkerhet ska vara systematiskt och långsiktigt.

## Informationssäkerhetspolicy

Denna policy innehåller Public Peoples viljeinriktning och övergripande mål för informationssäkerhetsarbetet. Policyn gäller hela bolagets verksamhet, styrelsen och samtliga anställda.

## Bakgrund

Behovet av informationssäkerhet ökar i takt med att kommunikationen effektiviseras, självbetjäningen utökas med hjälp av olika e-tjänster samt genom direktkontakt. I allt större utsträckning sker också användning av systemstöd för att leverera tjänster på ett effektivt sätt. Kunder, kandidater, medarbetare och samarbetspartners ska kunna förvänta sig att Public People hanterar information som rör dem, exempelvis personuppgifter och information om de olika tjänster de använder, på ett säkert sätt.

Konsekvensen av bristande informationssäkerhet kan medföra störningar i verksamheter, att information går förlorad, förvanskas eller rent av stjäls. Det kan även medföra ekonomiska förluster och att förtroendet för eller varumärket Public People påverkas negativt.

## Informationssäkerhet

Informationssäkerhet omfattar alla informationstillgångar inom hela bolagets verksamhet utan undantag, oavsett om den behandlas manuellt eller automatiskt och oberoende av vi vilken form eller miljö den förekommer. Då stora delar av informationen hanteras med hjälp av IT-system handlar informationssäkerhet även om teknik.

*Definition av informationssäkerhet*

- **Riktighet** – Informationen ska vara tillförlitlig, korrekt, aktuell och fullständig.
- **Sekretess** – Att information i dokument, system och handlingar inte görs tillgängliga eller avslöjas för obehörig.
- **Spårbarhet** – Att i efterhand kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt ex. handling, användare, dator, skrivare eller system.
- **Tillgänglighet** – Att information är tillgänglig i skälig och förväntad utsträckning och inom rimlig tid.

## Övergripande målsättning

En god informationssäkerhet syftar till att säkra en effektiv informationsförsörjning och att undgå fel som påverkar möjligheterna att bedriva en ändamålsenlig verksamhet. Arbetet med informationssäkerhet ska vara systematiskt och långsiktigt. Genom att säkerställa en god nivå av systematiskt informationssäkerhetsarbete möjliggörs att lagkrav följs, kritisk verksamhet upprätthålls, informationsläckage förhindras, kontroll av kostnader uppnås, förtroendet för bolagets tjänster och varumärke skyddas.

## Långsiktiga målområden

- Informationsförsörjningen ska vara säker, effektiv och bidra till stöd åt verksamheten.
- Informationssäkerhetsarbetet sker enhetligt och systematiskt.
- Samtliga informationstillgångar ska vara identifierade och förtecknade. Av förteckning ska framgå vem som är informations-eller systemägare.
- Medarbetare ska ha kunskap om gällande informationssäkerhetsregler som rör det egna tjänstestället och de informationssystem/rutiner som där används.
- Händelser i informationssystemen som kan leda till negativa konsekvenser för bolagets åtaganden ska identifieras, åtgärdas och förebyggas.
- Informationssäkerhetsarbetet ska följa standarderna ISO/IEC 27001 och ISO/IEC 27002.

## Roller och ansvar

Alla har ett ansvar för att säkerheten fungerar. Den som upptäcker brister i datasäkerheten måste uppmärksamma sin chef på det. Alla medarbetare måste också rapportera händelser som kan göra att våra informations-tillgångar utsätts för risker. Verksamhetsansvariga ska planera, genomföra och återrapportera informationssäkerhetsarbetet. Chefer har ett ansvar att informera sina medarbetare om policyn för informationssäkerhet och dess tillämpningar.

*Följande roller är centrala för det strategiska och operativa informationssäkerhetsarbetet på Public People:*

### Ledning och verkställande direktör

Ytterst ansvarig för Public Peoples information och dess säkerhet och riktighet. Har till uppgift att följa upp efterlevnad i verksamheten och eventuella incidenter. Ansvarar även strategiskt och operativt för informationssäkerhetsarbetet samt för att se över och eventuellt revidera informationssäkerhetspolicyn.

### Informationsanvändare

Informationsanvändare är alla som hanterar information, oavsett i vilken form den finns, vilket inkluderar anställda så väl som icke anställda. Ansvarar för att ha kunskap om och följa policy, riktlinjer och rutiner för informationssäkerhet inom Public People. Ansvarar också även för att information som hen själv skapar skyddas på det sätt som informationsägaren bestämt.

### Informationsägare

All information ska ha en utsedd informationsägare. Om rollen inte har delegerats är det personalansvarig chef som ansvarar för informationen som också är informationsägare. Ansvarar för att värdera informationen och därigenom ställa krav på dess skydd.

PUBLIC PEOPLE

Vi gör skillnad för offentlig sektor

PUBLICPEOPLE.SE