



# Informationssäkerhetspolicy YrkesAkademin

# Dokumentinformation

## Revisionshistorik

Datum	Version	Ansvarig	Kommentar
2019-10-17	1.0	VD	Beslutad i YrkesAkademin styrelse

## Egenskaper

Dokumenttyp	Giltighet	Användning
Styrande	Tillsvidare	Internt

## Relaterade dokument

Ref#	Dokument	Kommentar

# Informationssäkerhetspolicy

## Bakgrund

God informationssäkerhet är en investering samt en billig försäkring och genom att utgå från verksamhetens behov av skyddsnivå kan informationssäkerhetsarbetet ständigt förbättras samt bidra till rätt säkerhetsskydd för troliga och oönskade framtida händelser.

## Syfte

Denna policy anger inriktning och övergripande mål samt säkerställande av ett strukturerat, riskbaserat och konsistent informationssäkerhetsarbete på koncernen YrkesAkademin.

Syftet är att skydda informationstillgångar från alla typer av hot, såväl externa som interna.

## Omfattning

Policyn gäller för alla anställda, konsulter, leverantörer och andra tredjepartsanvändare som på något sätt är involverade i verksamheten.

## Informationssäkerhet

Informationssäkerhet omfattar YrkesAkademin:s verksamhet och all information utan undantag oavsett den hanteras i cyberrymden, i datorer, i ett telefonsamtal eller på ett papper.

Då stora delar av informationen hanteras med hjälp av IT-system handlar informationssäkerhet även om att kravställa hur våra tekniska lösningar skall fungera.

## Mål

YrkesAkademin har följande mål med sitt informationssäkerhetsarbete:

- Informationsförsörjningen skall vara säker, effektiv och bidra till stöd åt verksamheterna.
- Informationssäkerhetsarbetet skall ske enhetligt och systematiskt som en naturlig del av verksamheten.
- Personal skall ha kunskap kring gällande informationssäkerhetsreglemente och kopplat till de informationssystem/rutiner som används.
- Informationssäkerhetsarbetet skall följa standarderna ISO/IEC 27001 och ISO/IEC 27002.
- Koncernövergripande rutiner, regler och anvisningar skall upprättas.
- Alla informationstillgångar skall klassificeras enligt framtagen modell.
- Samtliga informationstillgångar skall vara identifierade och dokumenterade med informations- och systemägare.
- Händelser i informationssystemen som kan leda till negativa konsekvenser skall identifieras, åtgärdas och förebyggas.
- Kontinuitetsplanering skall genomföras för varje informationstillgång för att säkerställa förmåga att bedriva verksamheten på acceptabel nivå under normala förhållanden.

# Ansvar

## Övergripande

Informationssäkerhetsarbete bygger på delaktighet och tydlig ansvarsfördelning samt varje anställds bidrag att tillsammans bygga en säkerhetskultur.

Yttersta ansvaret för informationssäkerheten på YrkesAkademin ligger hos VD.

De beslut som fattas av Dataskyddsombudet för att åtgärda överträdelser av dataskydd måste upprätthållas av företagets ledning.

## IT chefs ansvar

- Arbetet med denna policy och underordnade handlingar
- Säkerställa kommunikation och utbildning kring informationssäkerhetsarbetet för alla som omfattas av policy och underliggande dokument.

## Linjechefers ansvar

- Chefer på alla nivåer har det operativa ansvaret för inom deras avdelning att denna policy med underliggande dokument introduceras och efterlevs.

## Medarbetarens ansvar

- Alla anställda är individuellt ansvariga för att tillämpa reglerna och för att rapportera eventuella överträdelser, incidenter eller brister i dataskyddet

## Efterlevnad

- Eventuella brott mot denna policy kan leda till disciplinära åtgärder.
- Alla incidenter ska registreras och rapporteras samt övervakas kontinuerligt för att identifiera och minimera risker.