

# Informations- säkerhetspolicy

Kontakt: Linus Lindström, chef IT, E-post: [linus.lindstrom@vasakronan.se](mailto:linus.lindstrom@vasakronan.se)

## Inledning

Information är en av Vasakronans viktiga tillgångar och behöver hanteras på ett säkert sätt. Vårt informationssäkerhetsarbete omfattar de åtgärder vi vidtar för att skydda vår information och säkerställa att den uppfyller krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Policyn för informationssäkerhet syftar till att minska risken för dataintrång, felaktig hantering och andra säkerhetsshot. En säker hantering av information stärker inte bara vårt eget skydd utan även våra kunders.

## Mål och syfte

Målet med informationssäkerhetsarbetet är att skydda alla Vasakronans informationstillgångar. Informationssäkerhetsarbetet ska skapa trygghet för medarbetare såväl som kunder och proaktivt förbereda oss för att hantera eventuella incidenter.

Vasakronans informationssäkerhetsarbete ska vara systematiskt, strukturerat och riskbaserat. Syftet med arbetet är att säkerställa ett balanserat skydd som möjliggör att rätt information är tillgänglig för rätt personer vid rätt tidpunkt och förhindrar otillåten användning av information.



## Styrande principer

### Integrerat informationssäkerhetsarbete

Informationssäkerhetsarbetet ska vara en naturlig del av det dagliga arbetet inom hela vår verksamhet och stödja oss i att uppnå våra verksamhetsmål och upprätthålla ett högt förtroende. Vid behov av mer konkreta och detaljerade regleringar ska kompletterande instruktioner eller rutiner implementeras på aktuell enhet/avdelning.

### Riskbaserat informationssäkerhetsarbete

De åtgärder som vi vidtar för att skydda vår information ska baseras på risker som identifieras i verksamheten. Arbeta med risker ska vara kontinuerligt och nya bedömningar ska göras på minst årsbasis. En prioriterad riskbild ska sedan ligga till grund för det fortsatta informationssäkerhetsarbetet.

### Strukturerat och proaktivt

Vårt informationssäkerhetsarbete ska vara välorganiserat, proaktivt och ständigt förbättras, med målet att det ska vara enkelt att göra rätt.

### Balanserade skyddsåtgärder

När vi väljer skyddsåtgärder för att minska risker till en acceptabel nivå ska dessa åtgärder balanseras mellan skyddsvärde, hotbild, risknivå, verksamhetspåverkan och kostnad.

### Tillgång till information

Tillgång till information ska baseras på de behov som finns kopplade till våra arbetsuppgifter. Information är en central del i vårt arbete och tillgång till rätt information i rätt tid är avgörande för



vår affär. Men genom att inte ha tillgång till mer information än vi behöver bidrar vi till att upprätthålla en bra skyddsnivå. Genom klassning av information vägleder vi vilken information som vi har tillgång till.

### **Incidentrapportering**

Incidenter och avvikelser ska rapporteras omgående och hellre en gång för mycket än en gång för lite. De ska hanteras enligt en strukturerad process så att vi proaktivt kan hantera och förebygga förlust och skador.

### **Informationssäkerhetskultur**

Vi ska skapa en stark informationssäkerhetskultur där all personal har den medvetenhet och kunskap som krävs för att upprätthålla säkerheten över tid.

### **Roller och ansvar**

Samtliga medarbetare på Vasakronan bär ett ansvar att följa denna policy. I arbetet med att integrera informationssäkerhet som en naturlig del av vårt arbete och erbjudande bär alla medarbetare ett stort ansvar för informationssäkerheten på Vasakronan.

Företagsledningen ansvarar för att säkerställa att informationssäkerhetsarbetet på Vasakronan bedrivs i enlighet med lagkrav och åtaganden som bolaget har.

Chef IT, som rapporterar till bolagets chef för Ekonomi och Finans är Vasakronans utpekade ansvarige för informationssäkerhet med den centrala rollen att leda, samordna och övervaka informationssäkerhetsarbetet. Chef IT säkerställer efterlevnad av lagkrav, bolagets styrdokument för informationssäkerhet, kommunikation av policy till ledning och chefer, informationsinsatser och utbildningar.