



INFORMATION- SÄKERHETSPOLICY



Informationssäkerhetspolicy 2021

1. INTRODUKTION OCH SYFTE

Vectura är ett fastighetsbolag som skapar värde för människor, företag och samhälle genom att utveckla platser och upplevelser. Vi verkar i hela värdekedjan, vilket innebär att vi är en långsiktig partner under hela resan från markköp och förvärv till projektering och förvaltning.

I allt vi gör utgår vi från våra värderingar. Det innebär att vi alltid är:

- Engagerade
- Proaktiva
- Nyskapande
- Långsiktiga

Vecturas arbete med informationssäkerhet ska bidra till att nå de mål som satts upp för vår verksamhet. I detta ingår att säkerställa att vårt arbete sker med hög kvalitet och informationssäkert. En effektiv och säker användning av information är en förutsättning för att upprätthålla förtroendet för Vecturas verksamhet.

Arbetet med informationssäkerhet ska ge Vectura en förmåga att identifiera risker och sårbarheter som har med information att göra samt att införa säkerhetsåtgärder som minskar riskerna till en acceptabel nivå. Informationssäkerhetsarbetet ska vara integrerat i Vecturas verksamhet.

Med informationssäkerhet menas att bibehålla *konfidentialitet*, *riktighet*, *tillgänglighet* och *autenticitet*:

- **Konfidentialitet** – att informationen är tillgänglig endast för dem som är behöriga.
- **Riktighet** – att informationen skyddas mot oavsiktlig och avsiktlig förvanskning.
- **Tillgänglighet** – att säkerställa att användarna har tillgång till informationen när de behöver den.
- **Autenticitet** – att information kan spåras och återskapas.

All hantering av skriftlig och elektronisk information ska skyddas, dvs. kopiering, distribution, förändring, läsning, makulering, förvaring och arkivering.

Vecturas informationssäkerhetsarbete ska bedrivas med utgångspunkt i Svenska Institutet för Standarder (SIS) som avser informationssäkerhet SS-ISO/IEC 27001 och 27002¹.

2. ROLLER OCH ANSVAR

Policyn omfattar alla medarbetare och alla delar av Vecturas verksamhet. Samtliga medarbetare förväntas aktivt söka och ta till sig information samt förstå hur de i sin roll i verksamheten påverkar och bidrar till att uppnå Vecturas informationssäkerhetspolicy och mål.

VD fastställer Vecturas principer för informationssäkerhet, affärsplan och budget.

Ledningen ansvarar för implementering och arbetsfördelning av det operativa informationssäkerhetsarbetet i organisationen.

¹ <https://www.sis.se/iso27000/dettariso27000/>

Uppföljning och utvärdering av arbetet görs årligen. Resultaten styr valet av skyddsåtgärder. Identifierade risker ska hanteras genom att reduceras, elimineras eller accepteras.

Styrelsen fastställer policyn och gör en återkommande årlig bedömning av policyns aktualitet samt beslutar om eventuella revideringar.

Ledningen har ansvar för informationssäkerheten inom sitt ansvarsområde genom uppföljning och systematiskt arbete, med åtgärder och val som anpassas efter verksamhetens behov, legala krav och rådande hotbild. Ledningen säkerställer att personalen utbildas och informeras för att åstadkomma ett högt medvetande på området.

- Allt informationssäkerhetsarbete ska vara baserat på principen ständiga förbättringar och årlig uppföljning.
- All personal (anställda/inhyrda) ska vara informerade och medvetet använda policyn och principer för Vecturas informationstillgångar.
- Riskanalys ska användas i det dagliga arbetet och hanteringen av informationstillgångar.
- All kritisk information ska vara identifierad klassificerad och ha ansvarig utsedd.
- All information ska klassificeras och hanteras enligt gällande princip.
- Alla misstänkta informationssäkerhetsincidenter ska rapporteras.
- För affärskritisk information ska det finnas kontinuitetsplaner.

2.1 IT

- IT är outsourcad och köps som tjänst

IT-funktionen – köps som tjänst och levereras via molntjänster, som hanteras av valda partners. Vectura ställer krav och avtalar in informationssäkerhet i leverantörernas leverans, vilket omfattar allt arbete som *IT-funktionen* gör, oavsett egen personal, leverantörer eller molntjänster. *IT-funktionen* och *IT-systemägare* ansvarar för att en systemförteckning finns över aktiva system.

IT-ansvarig – ska vara utsedd av Vecturas ledning, och driver och samordnar Vecturas arbete med *IT-funktionen*.

IT-systemägare – är en anställd på Vectura som hanterar kontakten med *IT-funktionen* för ett specifikt system. *IT-systemägaren* klassar informationen ur ett informationssäkerhetsperspektiv, inklusive personuppgifter. *IT-systemägaren* genomför riskanalyser, ansvarar för vilka behov, åtgärder och krav som behöver ställas på *IT-funktionen* samt att nödvändiga åtgärder införs.

IT-ansvarig är *IT-systemägare* för den gemensamma molntjänsten Office 365.

3. KLASSNING OCH SKYDD AV INFORMATION

3.1 Syfte och omfattning

Syftet är att känslig och/eller sekretessbelagd information inte ska röjas.

Kravet på informationsklassning omfattar all information som kommer in till eller skapas inom Vectura. Information klassas för att verksamheten ska kunna hantera informationen med rätt säkerhet. Klassningen ska göras med avseende på *konfidentialitet, riktighet och tillgänglighet*.

3.2 Modell för klassning

Klassningsmodellen är ett verktyg för att sätta lämplig säkerhetsnivå när nya IT-system förändras, utvecklas anskaffas eller används.

Vid behov ska klassningen omprövas och förändras över tid.

Tre informationsklasser ska användas för klassning av informationstyper.

Klass/ konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet
Mycket känslig – allvarlig	Förlust av <i>konfidentialitet</i> innebär allvarlig negativ påverkan på egen/annans organisation/person.	Förlust av <i>riktighet</i> innebär allvarlig negativ påverkan på egen/annans organisation/person.	Förlust av <i>tillgänglighet</i> innebär allvarlig negativ påverkan på egen/annans organisation/person.
Känslig	Förlust av <i>konfidentialitet</i> innebär negativ påverkan på egen/annans organisation/person.	Förlust av <i>riktighet</i> innebär negativ påverkan på egen eller annans organisation/person.	Förlust av <i>tillgänglighet</i> innebär negativ påverkan på egen/annans organisation/person.
Öppen – ej känslig eller försumbar	Inte finns något krav på <i>konfidentialitet</i> , eller där förlust medför försumbar/ingen skada alls för egen/annans organisation/person.	Inte finns något krav på <i>riktighet</i> , eller där förlust medför försumbar/ingen skada alls för egen/annans organisation/person.	Inte finns något krav på <i>tillgänglighet</i> , eller där förlust medför försumbar/ingen skada alls för egen/annans organisation/person.

4. FÖREBYGGA OCH ÅTGÄRDA

För att förebygga incidenter arbetar vi informativt inom organisationen för att samtliga medarbetare ska ha en medvetenhet kring samtliga policyer och koder. Vid en eventuell incident som avser ovan vänder medarbetaren sig i första hand till närmaste chef, VD och HR för stöd.

5. REVISIONSHISTORIK

Revision	Datum	Uppdaterad av	Godkänd av	Revisions Information
Första release	2021-06	Joel Ambré	Styrelsen Vectura Fastigheter AB	Första release