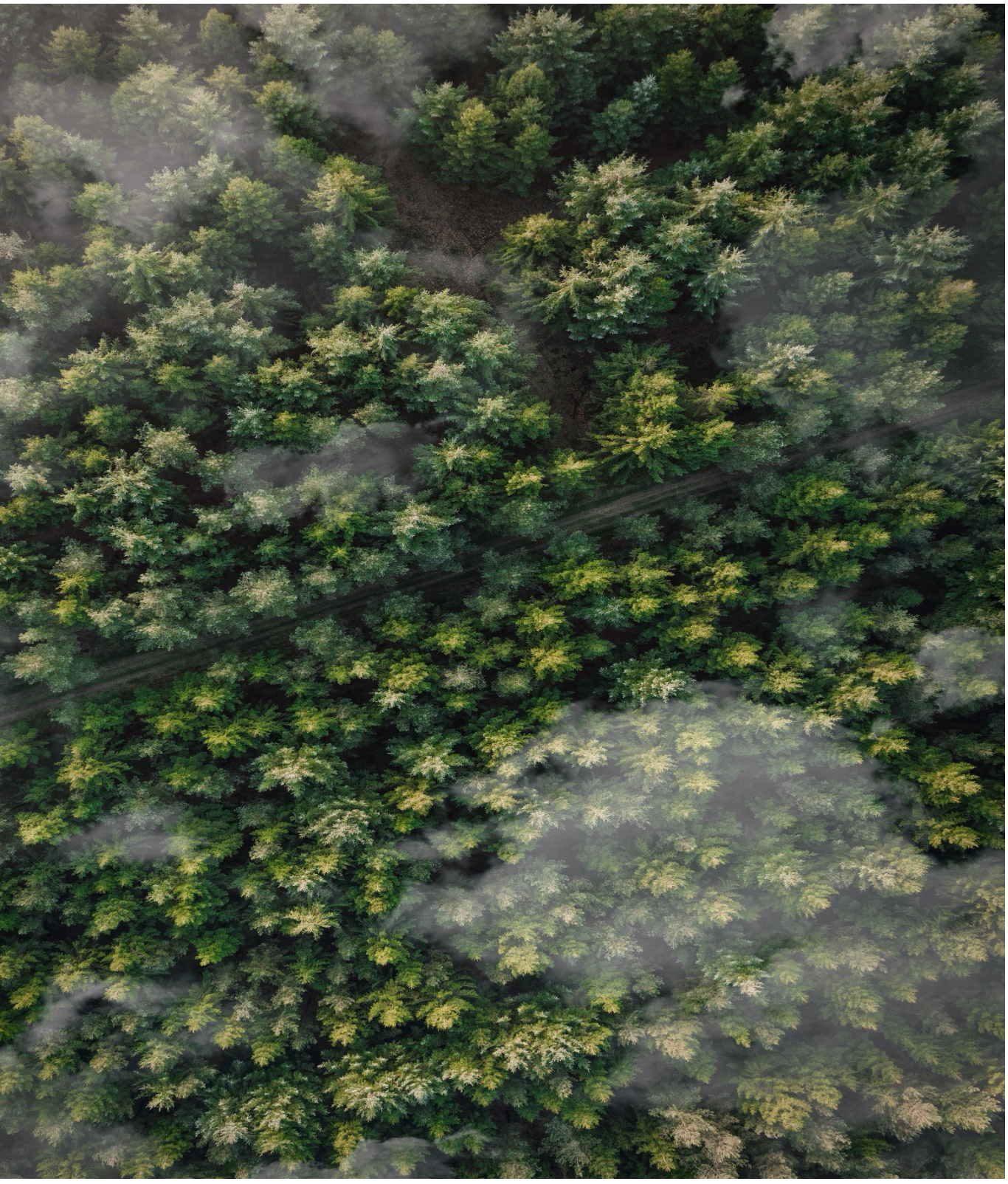
VECTURA FASTIGHETER AB
RIDDARGATAN 10
114 35 STOCKHOLM

2026
VECTURA.SE

INFORMATIONSSÄKERHETSPOLICY – VECTURA FASTIGHETER AB



Materialet är konfidentiellt och får inte spridas utanför Vectura utan godkännande av VD eller IT-chef.

Vectura

Informationssäkerhetspolicy

Innehåll

Informationssäkerhetspolicy 3

1. Syfte och omfattning 4
Hållbarhet 4
Innovation 4

2. Roller och ansvar 4

3. Grundläggande principer 4

4. Mediahantering 4

5. Vecturas presstalespersoner 4

6. Fysisk & miljömässig säkerhet 5

7. Skydd av klient- och mobilenheter 5

8. IT-säkerhet 5

9. Identitet och åtkomst 5

10. Informationshantering och personlig integritet 5

11. Säker användning och utbildning 5

12. Riskhantering 6

13. Incidenthantering 6

14. Driftskontinuitet och backup 6

15. Efterlevnad och revision 6

16. Undantag, dispens och policyförvaltning 6

17. Relaterade dokument 6

18. Revidering 6

1. SYFTE OCH OMFATTNING

Denna policy beskriver hur Vectura skyddar all information – digital, fysisk och muntlig – så att konfidentialitet, riktighet och tillgänglighet upprätthålls i enlighet med lag, avtal och affärsmål. Policyn täcker både informations- och cybersäkerhet. Policyn gäller samtliga anställda, konsulter, leverantörer och partners som hanterar Vecturas information eller IT-resurser. Med Vectura avses i denna policy Vectura Fastigheter AB samt dotterbolag. Personer anställda i dotterbolag som har åtkomst till Vecturas IT-resurser eller information omfattas av samma regler som anställda i moderbolaget.

Hållbarhet

Vårt hållbarhetsarbete möjliggör ett långsiktigt värdeskapande där människa och miljö får stå i fokus. Vi gör detta genom att utveckla framtidssäkrade, flexibla fastigheter, som möter högsta kvalitetskrav, baserade på medvetna val och långsiktighet.

Innovation

Vectura strävar efter att med nyskapande lösningar och processer inom fastighetsutveckling, projektledning och byggteknik, leverera projekt som höjer standarden i branschen.

2. ROLLER OCH ANSVAR

- Styrelsen godkänner policyn och följer upp efterlevnad.
- Ledningsgruppen säkerställer resurser, kommunikation och implementering.
- IT-chef leder det operativa informationssäkerhetsarbetet, genomför riskanalys, revision och rapportering.
- Kommunikationsansvarig – ansvarar för bolagets externa kommunikation och mediahantering.
- Verksamhetsansvarig äger sitt respektive områdes processer, system- och information, klassificering av data, styr åtkomst och ser till att kontroller är på plats.
- Alla medarbetare följer policyn och rapporterar incidenter omedelbart.
- Organisatoriska skyddsåtgärder ska vara risk- och kostnadsanpassade.
- Dokumenterad ställföreträdare ska finnas för säkerhetsfunktionen (security@vectura.se) och dataskyddsfunktionen (gdpr@vectura.se) för att säkerställa kontinuitet vid frånvaro.

3. GRUNDLÄGGANDE PRINCIPER

- Ägarskap – all information ska ha en utsedd informationsägare i verksamheten.
- Godkända system – endast system som finns i Vecturas systemregister får lagra eller behandla Vecturas information.
- Balanserad säkerhet – tekniska och organisatoriska skyddsåtgärder ska vara risk- och kostnadsanpassade utifrån klassning och affärs-/lagkrav.

4. MEDIAHANTERING

För att säkerställa högsta kvalitet och effektivitet i mediehanteringen gäller denna policy för samtliga medarbetare på Vectura. Policyn hanterar rätten att uttala sig för Vecturas räkning och avser inte den enskildes grundlagsskyddade yttrandefrihet. För mer information om konfidentiell information och sekretess, finns information i respektive medarbetares anställningsavtal.

5. VECTURAS PRESSTALESPERSONER

Vectura har tre talespersoner vilka är de enda som alltid har rätt att uttala sig för Vecturas räkning i media; VD, kommunikationschef och kommunikationsansvarig. Övriga medarbetare har endast rätt att uttala sig för Vecturas räkning efter delegation av någon av deras ordinarie talespersoner.

6. FYSISK & MILJÖMÄSSIG SÄKERHET

Alla kritiska fysiska utrymmen, inklusive server- och nätverksrum samt arkiv, ska skydda med passerkontroll och vid behov kameraövervakning och brandskydd.

7. SKYDD AV KLIENT- OCH MOBILENHETER

Datorer och mobila enheter ska alltid låsas när de lämnas obevakade. Vid arbete utanför kontoret ska åtkomst till organisationens tjänster alltid ske med multifaktorautentisering (MFA). Vid användning av publika nätverk rekommenderas extra försiktighet och säkerhetsmedvetenhet. Kryptering är obligatoriskt på mobila enheter. Stöld eller förlust rapporteras direkt och senast inom 24 timmar. Extern lagring bör undvikas och, om nödvändigt, ska enheten vara krypterad. Vecturas IT-enheter är centralt hanterade via MDM (Apple Business Manager och Microsoft Intune), vilket säkerställer att kryptering, säkerhetsuppdateringar och konfiguration följs och möjliggör fjärradering vid förlust eller stöld. Privata enheter (BYOD) får inte användas för Vectura-arbete. Detaljer finns i IT-riktlinjerna (2.3.4).

8. IT-SÄKERHET

Alla datorer och servrar följer Vecturas säkerhetsstandard. Nätverket är segmenterat och skyddat av brandväggar. Data på bärbara enheter och molntjänster ska alltid vara krypterade. Säkerhetsuppdateringar skall installeras utan onödigt dröjsmål och enligt leverantörens rekommendationer. IT-chefen ansvarar för uppdateringsplan, test och rapportering.

9. IDENTITET OCH ÅTKOMST

Multifaktor-autentisering är obligatoriskt. Åtkomst styrs via roller och privilegierade rättigheter är tidsbegränsade. Åtkomstloggar sparas **minst 3 år** eller längre när det krävs enligt gällande lagar och branschkrav.

10. INFORMATIONSHANTERING OCH PERSONLIG INTEGRITET

Konfidentiell information och personuppgifter som rör leverantörer och medarbetare ska endast användas för avsett ändamål och behandlas med särskild aktsamhet. Vectura skyddar informationen med tekniska och organisatoriska säkerhetsåtgärder, exempelvis kryptering, åtkomstkontroller och regelbundna säkerhetsgranskningar.

IT-chefen ansvarar för att dessa skyddsåtgärder implementeras, följs upp och kontinuerligt förbättras. Personuppgifter lagras endast så länge som krävs för ändamålet eller enligt gällande lagstiftning, och all behandling sker i enlighet med GDPR samt företagets Integritetsriktlinjer. AI-verktyg räknas som informationsbehandling och omfattas av denna policy: personuppgifter, känsliga affärshemligheter och konfidentiell information får inte matas in i AI-verktyg utan att Vectura har personuppgiftsbiträdesavtal (DPA) på plats med leverantören. AI-genererad output ska behandlas som osäker information och kontrolleras av människa innan den används som underlag för beslut eller skickas till mottagare. Detaljerade regler för AI-användning finns i AI-riktlinjerna (2.3.3). Medarbetare ska bara ta del av den information som krävs för deras arbete (least privilege). Att avsiktligt tillskansa sig information utöver det – exempelvis genom att titta på en kollegas olåsta enhet, läsa post eller dokument som inte rör eget arbete eller försöka kringgå åtkomstkontroller – är inte tillåtet och hanteras som en säkerhetsincident enligt §13.

11. SÄKER ANVÄNDNING OCH UTBILDNING

Samtliga medarbetare följer IT-riktlinjerna. Alla genomgår årlig säkerhetsutbildning med kunskapskontroll och deltar regelbundet i övningar för att upptäcka och förebygga säkerhetshot. Medarbetare som använder AI-verktyg ska ha tillräcklig AI-kunnighet enligt artikel 4 i EU:s AI-förordning – det vill säga grundläggande förståelse för hur AI fungerar, dess begränsningar (hallucinationer, bias) och vilka data som inte får matas in. Denna utbildning sker enligt AI-riktlinjerna (2.3.3).

12. RISKHANTERING

Riskanalyser genomförs minst årligen och inför större förändringar för att säkerställa att skyddsåtgärder är relevanta och effektiva. AI-användning ska ingå i den allmänna riskanalysen, med särskilt fokus på datahantering, beroende av extern leverantör, tillförlitlighet i AI-output samt risk för diskriminering eller orättvisa beslut.

13. INCIDENTHANTERING

Anställda rapporterar misstänkta säkerhetsincidenter till security@vectura.se eller misstänkta personuppgiftsincidenter till gdpr@vectura.se – senast inom 24 timmar.

IT-funktionen tar emot ärendet, utreder tekniskt och gör en GDPR-bedömning tillsammans med dataskyddsfunktionen. Vid misstanke om medarbetares beteende kopplas HR in. IT-funktionen och HR bedömer gemensamt åtgärdsnivå innan respektive chef informeras och hanterar personalfrågan. Chefer utreder inte ärenden på egen hand.

Den som rapporterat ett ärende får alltid en bekräftelse vid mottagandet och ett avslutande besked när ärendet är hanterat.

Personuppgiftsincidenter hanteras av dataskyddsfunktionen i samråd med IT-funktionen, inklusive eventuell anmälan till Integritetsskyddsmyndigheten (IMY) inom 72 timmar enligt processen i Dataskyddspolicyn (2.3.5).

14. DRIFTSKONTINUITET OCH BACKUP

Det skall finnas dokumenterade kontinuitets- och återställningsplaner där mål för återställningstid och dataförlust fastställs per system utifrån risk- och kostnadsanalys. Geografiskt separerade säkerhetskopior ska finnas och planen testas och uppdateras minst två gånger om året.

15. EFTERLEVNAD OCH REVISION

Internkontroller utförs minst halvårsvis för att säkerställa efterlevnad av säkerhetskraven och upptäcka hot och brister. Penetrationstester och granskningar mot regelverk genomförs minst årligen.

16. UNDANTAG, DISPENS OCH POLICYFÖRVALTNING

Dispens från policyn beviljas av IT-funktionen under max 6 månader med krav på kompenserande åtgärder. Policyn ses över minst en gång per år och uppdateras vid behov.

17. RELATERADE DOKUMENT

- Integritetsriktlinjer - skydd av personuppgifter för externt bruk
- Dataskyddsriktlinjer – skydd av personuppgifter för internt bruk
- AI-riktlinjer - säker användning av AI.
- IT-riktlinjer - användning av IT-utrustning och system.

18. REVIDERING

Policyn revideras och godkänns av styrelsen minst en gång per år eller vid behov av förändringar. Ansvarig för uppdatering anges tydligt vid varje revision.

- 2021 – Joel Ambré
- 2022 – Joel Ambré
- 2023 – Petter Ekevärn
- 2025 – Ulrica Sjöswärd
- 2026 – Ulrica Sjöswärd