Informationssäkerhetspolicy C4 Hus AB

Introduktion

Denna policy reglerar skyddet av C4 Hus AB:s informationstillgångar mot eventuella hot – interna eller externa, avsiktliga eller oavsiktliga. Med informationstillgångar menas både information (data) som sådan och de resurser som används för att hantera informationen (IT-system, nätverk, servrar och arbetsstationer inklusive mobila enheter som surfplattor och mobiltelefoner).

Syfte och utgångspunkter

Syftet med denna policy är att säkerställa att all information hanteras på ett säkert och effektivt sätt. Information är en av C4 Hus AB:s nyckelresurser. Genom att arbeta systematiskt med informationssäkerhet utifrån etablerade standarder och genomtänkta policyer kan C4 Hus AB åstadkomma bättre kvalitet i verksamheten och ökad trovärdighet.

Arbetet med informationssäkerhet ska ta sin utgångspunkt i följande principer:

- **Tillgänglighet**. Våra medarbetare, kunder, partners och övriga intressenter ska ha tillgång till den information de behöver, när de behöver den och på förväntat sätt.
- **Riktighet**. Vår information ska vara korrekt och tillförlitlig. Informationen ska skyddas mot oönskade förändringar och fel.
- **Konfidentialitet/sekretess**. Vår information ska inte göras tillgänglig för eller avslöjas för obehöriga.
- **Spårbarhet**. Aktiviteter ska kunna härledas i efterhand. Vi ska kunna visa vad som har hänt och vem som har gjort vad i våra informationssystem.

C4 Hus AB:s arbete med informationssäkerhet ska ske utifrån etablerade standarder och internationella riktlinjer. Arbetet ska utföras på ett strukturerat sätt i enlighet med denna policy och C4 Hus AB:s övriga fastställda riktlinjer och rutiner.

Säkerhetsarbetet ska resultera i kostnadseffektiva och behovsanpassade säkerhetsåtgärder som harmoniserar med C4 Hus AB:s uppgift och verksamhetsmässiga åtaganden. Det ska ske på ett sätt som bidrar till att leverera kvalitet i verksamheten. Åtgärder för att säkra informationen ska i så liten utsträckning som möjligt vara ett hinder för utvecklingen av olika tekniska lösningar.

Skyddet av information ska tillgodose de krav som ställs på C4 Hus AB – både genom gällande lagstiftning och i överenskommelser med C4 Hus AB:s kunder, samarbetspartners och övriga intressenter.

Övergripande roller och ansvar

Policyn gäller för samtliga anställda och konsulter inom C4 Hus AB samt övriga kontraktsbundna intressenter. Var och en har ansvar för att skydda den information som man disponerar över utifrån givna riktlinjer och instruktioner.

Ansvaret för informationssäkerheten hos C4 Hus AB kan delas in i olika delar, huvudsakligen fysisk säkerhet, IT-säkerhet samt säkerhet för personuppgifter. Denna övergripande informationssäkerhetspolicy kompletteras med specifika styrdokument och riktlinjer inom dessa

områden. För mer detaljerad information hänvisas till C4 Hus AB:s separata IT-policy och dataskyddspolicy.

Följande personer har särskilt ansvar för delar av arbetet med informationssäkerhet:

- Carola Carlsson – Personuppgiftskoordinator
  Ansvarar för: Övergripande säkerhetsadministration, policydokument och internutbildning

Generella riktlinjer

Informationsklassning och riskbedömning

För att avgöra vilket skydd som behövs och hur olika typer av information får hanteras, ska känslig och/eller väsentlig information som hanteras inom C4 Hus AB klassificeras. Tillsammans med klassificeringen ska riskbedömningar avgöra vilka säkerhetsåtgärder som behövs för respektive informationstyp. Riskbedömningar ska genomföras löpande samt alltid vid större förändringar.

Åtkomst och behörighet

Information i IT-system ska alltid skyddas med antingen någon form av autentisering eller genom kryptering. C4 Hus AB ska arbeta aktivt med behörigheter i IT-system och göra medvetna bedömningar av vilka användare som ska ha tillgång till systemen, för att minskar mängden information som exponeras till olika användargrupper. Vi strävar alltid efter att minimera breda behörigheter, så att endast personer som i sin roll behöver tillgång till information har åtkomst till den. C4 Hus AB ska tillämpa rollbaserad åtkomstkontroll. Alla beslut och inställningar som rör användaråtkomst ska regleras centralt i IT-miljön.

Anställda, konsulter och övrig kontraktsbunden personal får inte ta del av eller bereda sig tillgång till företagets information utifrån privata intressen.

Loggning och uppföljning

Uppföljning och kontroll, bland annat genom granskning av loggar, ska vara en naturlig del i C4 Hus AB:s säkerhetsarbete. Det ska finnas rutiner för att övervaka loggar kontinuerligt och ett ändamålsenligt system där man kan söka fram händelser och granska loggar på ett effektivt sätt.

Säkerhetsincidenter

Den som upptäcker brister i informationssäkerheten måste uppmärksamma sin chef eller säkerhetsfunktionen på det. Alla medarbetare måste också rapportera händelser som kan göra att våra informationstillgångar utsätts för risker. Alla incidenter som sker ska alltid dokumenteras genom en incidentrapport som upprättas hos ansvarig avdelning.

Ett strukturerat arbete med incidenthantering ger möjligheten till kontroll och uppföljning av C4 Hus AB:s säkerhetsarbete och också stora möjligheter för organisationen att förebygga eller minska effekten av framtida incidenter.

Utöver en etablerad process för incidentrapportering, ska C4 Hus AB ha en framtagen plan för hur verksamheten ska kunna upprätthållas och återställas i händelse av en allvarlig incident eller kris. Riktlinjer och rutiner för hur C4 Hus AB säkerställer kontinuitet i affärskritiska verksamheter skapas och definieras av IT-avdelningen.

Outsourcing

Även för sådana system och tjänster som är outsourcade till extern leverantör så kvarstår en skyldighet hos C4 Hus AB att säkerställa att leverantören lever upp till lämplig säkerhet och följer överenskomna instruktioner.

Revidering av dokumentet

Denna policy ska revideras vid behov i samband med förändringar i verksamhetens inriktning och omfattning. En allmän översyn av dokumentet ska göras i samband med den årliga revisionen. I samband med revideringen ska också kompletterande riktlinjer och rutinbeskrivningar revideras på motsvarande sätt.

Denna policy har tagits fram av IT-avdelningen den 2021-10-21.

Frågor som rör informationssäkerhetspolicyn besvaras av Carola Carlsson.

Policyn uppdaterades senast den 2022-03-01.