Ocab

IT-säkerhetspolicy

Syfte

Denna policy har tagits fram för att främja och utveckla verksamhetens syn på, och förståelse för, IT-säkerhet. IT-systemen ger möjlighet till effektivt arbete och är därför en viktig del av verksamheten. Men det innebär även risker då Oleter Sweden Holding AB för Ocab hanterar både personuppgifter och företagshemligheter i våra system, vilket gör att vi måste följa både lagstiftning och våra kunders krav.

Giltighet

IT-systemen är en tillgång men också ett ansvarsområde som varje medarbetare är med och ansvarar för. För att minimera och förebygga problem så är det viktigt att den anställde förstår vad detta ansvar innebär. Policyn gäller och berör alla personer som hanterar information och/eller data för Oleter Sweden Holding ABs och därmed Ocabs räkning och utrymme för egna tolkningar eller tillämpningar finns inte. Informationstillgångar avser all information oavsett om den behandlas manuellt eller automatiskt och oberoende av i vilken form eller miljö den förekommer.

Mål

Det övergripande målet med säkerhetsarbetet inom IT är att säkerställa ett väl avvägt skydd för Ocabs data så att rätt åtkomst är tillgänglig för rätt person vid rätt tidpunkt och på ett spårbart sätt.

Zero Trust-principer:

- Etablera en nolltoleranspolicy för förtroende vid nätverksåtkomst och datahantering
- Införa autentisering på flera faktorer för alla användare, inklusive starka lösenord, biometrieller tokenbaserad autentisering
- Använda segmenteringstekniker för att dela upp nätverket i mindre zoner och begränsaåtkomst mellan dem
- Tillämpa kontinuerlig övervakning av användaraktivitet och nätverkstrafik för att upptäcka avvikelser och hot

Least Privilege-principer:

- Tillämpa principen om minsta privilegier genom att ge användare endast nödvändiga rättigheter för att utföra sina arbetsuppgifter
- Implementera en rollbaserad åtkomstkontroll (RBAC) för att styra vilka resurser och funktioner varje användare når baserat på deras befattning eller roll i organisationen
- Genomför regelbundna granskningar av användares behörigheter och ta bort onödiga privilegier

Ocab

Organisation och ansvar

Gällande centralt hanterade system äger systemägaren ansvaret och IT-avdelningen det grundläggande säkerhetsarbetet på IT-området och konsulterar systemägaren. IT-avdelningen jobbar kontinuerligt med utbildning och information till alla medarbetare för att hålla alla delaktiga i säkerhetsarbetet.

IT-avdelningen konsulterar, koordinerar, kontrollerar och rapporterar säkerhetsstatus. IT-avdelningen förbereder riktlinjer och procedurer.

Den enskilda anställda är ansvarig för att följa säkerhetspolicyn och att ta del av övriga riktlinjer och förhållningsregler kopplade till detta.

Säkerhetsrutiner

IT-avdelningen jobbar kontinuerligt med riskanalyser av hotbilder och med att säkerhetsställa IT-miljön till den högsta grad möjligt. Detta genom bland annat:

- Daglig backup av systeminformation, uppdateringar av system och andra typer avdrivrutiner vid behov. Kontinuerlig monitorering av våra system för både drift och säkerhetsrisker
- Kontroll av tillgång till nätverk via både fysiska- och mjukvarubrandväggar samt kryptering på samtliga företagsanslutna datorer
- Lösenordshantering enligt gällande standard samt användarhantering av information och systemåtkomster med spårbarhet

Rapportering

Samtliga medarbetare rapporterar IT-säkerhetsincidenter eller avvikelser till IT-avdelningen i supportportalen, enligt gällande riktlinjer som finns att tillgå i supportportalen.

IT-avdelningen informerar Ledningsgruppen om alla relevanta säkerhetsintrång. Den verkställande ledningen granskar säkerhetsstatusen årligen och rapporterar sedan till bolagsstyrelsen.

Överträdelse

Beroende på omfattning och eventuella resultat av överträdelsen, varierar konsekvenserna för detta från enkel tillsägelse till polisanmälan och eventuellt åtal.

Uppdateringar och granskningar

Denna policy kommer att granskas och uppdateras regelbundet för att säkerställa att den är aktuell och effektiv.

Senast uppdaterad 2024-04-24