Approved by: Elin Skörvald Li
Approved date: 2024-12-17

Ramudden

Informationssäkerhetspolicy

Riktlinjer för att hantera information på ett säkert sätt

Syfte
Denna policy syftar till att skydda företagets informationstillgångar mot interna och externa hot, säkerställa konfidentialitet, integritet och tillgänglighet, samt upprätthålla kundernas och medarbetarnas förtroende.

Omfattning
Policyn gäller alla anställda, konsulter, samarbetspartners och leverantörer. Den omfattar information med sekretessnivå ”publik”, ”intern” och ”förtrolig” som hanteras i företagets IT-system, mobila enheter, samt fysiska dokument. Policyn omfattar EJ hantering av uppgifter som har sekretessnivå ”*sekretess*” och ”*säkerhetsskyddad information*” där det finns separata styrdokument. För frågor kring detta uppmanas du kontakta Säkerhetsskyddschef på Ramudden.

Sekretessnivå	**Beskrivning**	**Berörs av denna Policy**
Publik	Publik information Öppen för alla	JA
Intern	Ramuddens interna information Öppen för all egen personal	JA
Förtrolig	Ramuddens interna information Öppen för begränsad del av egen personal	JA
Sekretess	Ramuddens interna information Öppen för strikt begränsad krets	NEJ, se Säkerhetsskyddsinstruktion
Säkerhetsskyddad information	Strikt hemlig information Öppen endast för säkerhetsprövad personal placerad i säkerhetsklass	NEJ, se Säkerhetsskyddsinstruktion

Omfattning
Företagsledningen har det övergripande ansvaret för informationssäkerheten. Säkerhetsskyddschef ansvarar för att implementera och övervaka denna policy, medan alla medarbetare är skyldiga att följa riktlinjerna.

Definition av informationssäkerhet
Informationssäkerhet innebär att skydda informationens konfidentialitet (skydd mot obehörig åtkomst), integritet (att säkerställa att information är korrekt) och tillgänglighet (att information är åtkomlig när den behövs).

Riktlinjer och principer
- **Konfidentialitet**: Endast behöriga personer får tillgång till känslig information.

- **Integritet**: Ändringar av information ska hanteras på ett sätt som säkerställer att de är korrekta och spårbara där det är relevant. För information klassad som ”Förtrolig” kan loggning och granskning tillämpas utifrån behov och risk.
- **Tillgänglighet**: System och information ska vara åtkomliga enligt affärsbehoven, med lämpliga åtgärder för att hantera störningar.

Riskhantering
Ramudden genomför regelbundna riskanalyser för att identifiera och bedöma hot mot informationstillgångar. Åtgärder vidtas för att minska riskerna, exempelvis genom tekniska skydd och utbildning av personal.

Åtkomstkontroll
Åtkomst till system och information är begränsad till de som behöver den för att utföra sitt arbete. Lösenord ska vara komplexa och bytas regelbundet. Multifaktorautentisering ska användas där det är möjligt.

Incidenthantering
Alla incidenter, såsom dataintrång eller informationsförlust, ska omedelbart rapporteras till Säkerhetsskyddschef. Incidenter ska dokumenteras och analyseras för att förhindra framtida händelser.

Utbildning och medvetenhet
Alla medarbetare ska genomgå utbildning i informationssäkerhet. Ny personal ska få en introduktion som inkluderar policy och riktlinjer.

Efterlevnad och uppföljning
Efterlevnad av denna policy kontrolleras regelbundet genom interna revisioner. Policyn ska revideras årligen eller vid behov för att säkerställa att den är aktuell.

Lagstiftning och standarder
Ramudden följer tillämplig lagstiftning, inklusive Dataskyddsförordningen (GDPR), bokföringslagen och andra regler som gäller för hantering av personuppgifter, elektronisk kommunikation och ekonomisk information.

Godkännande

Denna policy är godkänd av företagsledningen och träder i kraft från och med 2024-12-01