Diosentic

Informationssäkerhetspolicy

1. Inledning

Vi erbjuder socialtjänsten ett systematiskt och digitaliserat arbetssätt som mätbart förbättrar effektiviteten, kvaliteten, ekonomin och arbetsmiljön. Vi kallar det dioevidence™.

dioevidence™ ger er operativ fakta- och beslutsunderlag genom kartläggning, uppföljning och placeringsstöd inom alla socialtjänstens områden. Som operativt kan användas för att utveckla och leverera en mätbar bättre socialtjänst varje dag.

Vi vänder oss till socialtjänst som har ett ledarskap med tydliga ambitioner att utvecklas.

Diosentic Systems AB är engagerat i att skydda sina informationstillgångar och säkerställer att alla tjänster som tillhandahålls, inklusive molntjänster, uppfyller högsta standarder för informationssäkerhet. Denna policy är utformad för informationssäkerhet i molntjänster.

2. Syfte

Syftet med denna informationssäkerhetspolicy är att:
- Definiera riktlinjer och ansvar för informationssäkerhet inom Diosentic Systems AB.
- Skydda företagets och kundernas information mot obehörig åtkomst, förlust eller skada.
- Säkerställa efterlevnad av lagar och förordningar relaterade till informationssäkerhet och dataskydd.
- Främja en säkerhetsmedveten kultur bland alla anställda, underleverantörer och samarbetspartners.

3. Tillämpningsområde

Denna policy gäller för alla anställda, konsulter, underleverantörer och samarbetsparter som har tillgång till Diosentic Systems AB:s information och system, inkl. molntjänster.

4. Ansvar

- vd: Ansvarar för att säkerställa att informationssäkerhetspolicyn implementeras och efterlevs.
- Informationssäkerhetsansvarig: Ansvarar för att övervaka och rapportera om informationssäkerhetsrisker och incidenter.
- Anställda: Ansvarar för att följa säkerhetspolicyn, delta i kontroller och följa rutiner samt rapportera eventuella säkerhetsincidenter.
- Underleverantörer: Ansvarar för att följa säkerhetspolicyn, delta i kontroller och följa rutiner samt rapportera eventuella säkerhetsincidenter.

5. Riskhantering

Diosentic Systems AB genomför regelbundna riskanalyser för att identifiera och bedöma risker relaterade till informationssäkerhet, särskilt i samband med användning av molntjänster. Åtgärder vidtas för att hantera identifierade risker, inklusive tekniska och organisatoriska kontroller.

6. Informationsklassificering

All information som hanteras av Diosentic Systems AB klassificeras baserat på dess känslighet och betydelse. Klassificeringen styr hur informationen hanteras, lagras och skyddas, särskilt i molnmiljöer.

7. Åtkomstkontroll

Åtkomst till information och system begränsas till behöriga användare. Användare autentiseras och auktoriseras innan de får tillgång till känslig information. Detta inkluderar användning av

Diosentic

två-stegs autentisering för att öka säkerheten. Det är en viktig åtgärd för att motverka hot och säkerställa att endast behöriga användare får tillgång till företagets resurser.

8. Säkerhet i molntjänster

Diosentic Systems AB säkerställer att alla molntjänster som används uppfyller säkerhetskrav och standarder. Detta inkluderar:
- Datahantering: Känslig information krypteras både under överföring och lagring i molnet.
- Övervakning och loggning: Aktivitet i molntjänster övervakas och loggas för att identifiera och hantera säkerhetsincidenter.

9. Incidenthantering

Diosentic Systems AB har en tydlig process för att hantera informationssäkerhetsincidenter.

Alla incidenter rapporteras omedelbart och utreds för att förhindra framtida händelser i vårt digitaliserade incidenthanteringssystem. Incidenthanteringsprocessen inkluderar:

- Identifiering och klassificering av incidenter.
- Åtgärder för att hantera och återställa från incidenter.
- Rapportering och dokumentation av incidenter.

10. Utbildning och medvetenhet

Alla anställda genomgår regelbundna utbildningar i informationssäkerhet och medvetenhet om risker kopplade till molntjänster.

11. Efterlevnad och revision

Diosentic Systems AB genomför regelbundna digitaliserade revisioner för att säkerställa efterlevnad av denna informationssäkerhetspolicy och identifiera områden för förbättring.

12. Policyöversyn

Denna informationssäkerhetspolicy ses över och uppdateras minst en gång per år eller vid behov för att säkerställa att den förblir relevant och effektiv.

13. Godkännande

Denna informationssäkerhetspolicy har godkänts av ledningen för Diosentic Systems AB.

Denna policy är grundläggande och kan anpassas ytterligare för att passa specifika behov och krav inom Diosentic Systems AB.

Göteborg den 2 juni 2025

Thomas Kylander, vd