Sentinel Surveillance Systems

It-sikkerhedspolitik

Version 1.0

Klassifikation: Fortrolig mellem parterne

Sentinel Surveillance Systems, den 01. oktober 2025

1 Politik

Dette er Sentinel Surveillance Systems it-sikkerhedspolitik, der omfatter en beskrivelse af den overordnede informationssikkerhedspolitik, det valgte anvendelsesområde og principperne bag det implementerede sikkerhedsniveau.

1.1 Indledning

Sentinel Surveillance Systems it-sikkerhedspolitik skaber rammerne for et operationelt ledelsessystem for informationssikkerhed (ISMS), der udmøntes i etableringen af fastsatte retningslinjer for håndtering af Sentinel Surveillance Systems it-sikkerhed. Dermed etableres et grundlag for det daglige arbejde med it-sikkerhed i Sentinel Surveillance Systems. Ansvarsplacering, retningslinjer, risikohåndtering og it-beredskabsplaner er således emner, der reguleres under dette ledelsessystem.

Sentinel Surveillance Systems it-sikkerhed er baseret på:

- Almindeligt accepterede metoder og politikker for informationssikkerhed, herunder ”Best Practice” som beskrevet i den internationale standard ISO/IEC 27001

- Alle relevante regler, lovkrav, retningslinjer, vejledninger og kontrakter inden for Sentinel Surveillance Systems forretningsområde, databeskyttelsesloven, markedsføringsloven, statens krav og arbejdsmarkedsaftaler

1.2 Anvendelsesområde (Scope)

It-sikkerheden omfatter udvikling, levering og servicering af løsninger/produkter til Sentinel Surveillance Systems kunder, dvs. hele Sentinel Surveillance Systems og alle Sentinel Surveillance Systems aktiviteter.

1.3 Mål

Sentinel Surveillance Systems gennemfører alle nødvendige aktiviteter for at sikre:

- **Tilgængelighed:** At Sentinel Surveillance Systems forretningssystemer normalt er tilgængelige i forretningstiden / 24/7, og at der vedligeholdes et it-beredskab, som sikrer, at normal drift af forretningssystemerne kan reetableres indenfor 24 timer. Det sker bl.a. med brug af dublering (redundans) af systemer og forbindelser samt backup.

- **Integritet:** At man ved styring og manuelle inspektioner/kontroller af arbejdsgange, opnår en pålidelig og korrekt funktion af it-systemerne med pålideligt datagrundlag.

- **Fortrolighed:** At Sentinel Surveillance Systems informationer, herunder persondata og kundernes informatiner i Sentinel Surveillance Systems varetægt, kun er tilgængelige for de personer, og på den måde, som det er tiltænkt.

Sentinel Surveillance Systems risikovurderer virksomhedens forretningskritiske informationer og andre informationsaktiver, dels årligt, dels ved ændringer i trusselsbilledet, nye projekter, it-anskaffelser og behandlinger samt ved brud på sikkerheden. I forlængelse heraf vedligeholder Sentinel Surveillance Systems en risikohåndteringsplan.

Målsætningen er, at en tilstrækkelig og dokumenteret sikkerhed afvejes med ønsket om en hensigtsmæssig og brugervenlig anvendelse af it, så medarbejdere og kunder kan udføre deres opgaver på en optimal måde.

Sentinel Surveillance Systems gennemfører de aktiviteter, der er nødvendige for at holde medarbejderne orienterede om it-sikkerhed samt om deres ansvar over for virksomhedens informationer og systemer (awareness). Dette indbefatter, udover uddannelse af alle medarbejdere, introduktionsmateriale til nye medarbejdere, løbende mails og uddannelse om nye sikkerhedsudfordringer mv.

1.4 Ansvar

Ansvaret for den daglige styring af Sentinel Surveillance Systems it-sikkerhed er placeret hos ledelsen og risikoejere.

Hvis en medarbejder opdager trusler mod, eller brud på, informationssikkerheden, eller får mistanke om det, skal vedkommende straks underrette nærmeste leder om dette. I sidste ende er det den ansvarlige for den daglige styring af informationssikkerheden, som skal underrettes.

Medarbejdere, der bryder Sentinel Surveillance Systems informationssikkerhedspolitik, eller de heraf fastsatte procedurer og instruktioner, vil blive mødt med de forholdsregler, som Sentinel Surveillance Systems procedurer og personalepolitik foreskriver.

1.5 Opfølgning

Sentinel Surveillance Systems måler, vurderer og følger op på informationssikkerhedsområdet på følgende måde:

- Løbende opfølgning på hændelser inden for it-sikkerhed.
- Opfølgning på vidensniveau inden for it-sikkerhed i Sentinel Surveillance Systems i form af eksempelvis tests af medarbejdernes bevidsthed om it-sikkerhed (awareness- eller phishing-tests).
- Løbende vurderinger af sikkerhedsaspekter i forbindelse med nye projekter, anskaffelser og ændringer.
- Årlige gennemgange af risikovurderingerne og risikohåndteringsplanen.
- Gennemførelse af interne kontroller (auditeringer) og uafhængige tredjepartsevalueringer af informationssikkerheden i Sentinel Surveillance Systems.

På baggrund af dette gennemgår og revurderer ledelsen it-sikkerhedspolitikken en gang om året (review).

2 Godkendelse

Denne politik er vedtaget af Sentinel Surveillance Systems ledelse/bestyrelse den 1. oktober 2025

_____

Keld K. S. Ikker
CEO