Sentinel Surveillance Systems

Bilag 2 til it-sikkerhedspolitik
Retningslinjer for brugere
Version 1.0

Klassifikation: Fortrolig mellem parterne

Sentinel Surveillance Systems, den 01. oktober 2025

Hovedpunkter i it-sikkerheden

It-sikkerheden i Sentinel Surveillance Systems er baseret på disse retningslinjer.

1.1 Adgangsstyring

Udgangspunktet for tildeling af rettigheder og adgang til systemer og informationer er, at alt er låst ned og at der kun gives adgang, hvor der er et forretningsmæssigt behov.

Den daglige leder beslutter hvem, der skal have adgang til system og/eller informationer. Den it-ansvarlige tildeler herefter rettighederne ud fra disse beslutninger.

Sentinel Surveillance Systems servere og bærbare pc'er beskyttes med adgangskode og skærmlås samt opdaterede antivirusprogrammer og lokale firewalls. Bærbare pc'er med firmadata, herunder persondata, beskyttes desuden med kryptering).

Styring af adgangskoder følger Best Practice - minimum 15 karakterer, kombination af store/små bogstaver samt tal og specialtegn, med skift hver tredje måned.

Sentinel Surveillance Systems øvrige mobile enheder (mobiltelefoner og evt. tablets) beskyttes med en pinkode og brug af kryptering af firmadata samt mulighed for sletning (remote-wipe) af enhederne.

Sentinel Surveillance Systems fysiske lokaler er sikret med adgangssystem og forskellige alarmer. Den daglige leder beslutter hvem, der skal have adgang til hvad.

1.2 Informationer

Sentinel Surveillance Systems informationer findes på eksempelvis pc'er, servere, tablets, smartphones, usb-nøgler, cloud-lagre og lignende. Sikkerhedspolitikken kræver, at Sentinel Surveillance Systems informationer er beskyttet i tilfælde af tab, tyveri, kopiering mv., f.eks. med kryptering.

Medarbejdere i Sentinel Surveillance Systems må som udgangspunkt ikke opbevare firmarelaterede data i et cloud-lager, som Dropbox, med mindre dette er stillet til rådighed af Sentinel Surveillance Systems, eller godkendt af Sentinel Surveillance Systems ledelse til firmabrug. Hvis der opstår et akut behov for at opbevare firmarelaterede data i et ikke-godkendt cloud-lager, er det medarbejderens ansvar at sørge for, at data er krypterede.

1.3 Dokumentation

Sentinel Surveillance Systems it-sikkerhedspolitik, klassifikation og andre retningslinjer samt vejledninger er tilgængelige på Sentinel Surveillance Systems intranet.
Disse dokumenter vedligeholdes af den dagligt ansvarlige for Sentinel Surveillance Systems it-sikkerhed og godkendes af ledelsen.

1.4 Driftsikkerhed

Logning af aktiviteter er slået til i Sentinel Surveillance Systems systemer, og hvor der er persondata logges adgang og forsøg på adgang til de enkelte informationer også.

Sentinel Surveillance Systems opretholder funktionsadskillelse hvor muligt. Som minimum kræves (ligesom det er tilfældet ved betalinger i netbanken), at en anden person, f.eks. en fra ledelsen, medvirker ifm. godkendelse af større ændringer og ved tildeling af administratorrettigheder.

1.5 Klassifikation

Sentinel Surveillance Systems benytter følgende klassifikationer af informationer:

Offentlig – må ses/tilgås af alle.

Fortrolig – må ses/tilgås af alle i Sentinel Surveillance Systems og hos specifikke kunder/samarbejdspartnere.

Internt – må ses/tilgås af alle i Sentinel Surveillance Systems, men ingen udenfor

Følsomt – må kun ses/tilgås af en mindre gruppe med et konkret forretningsmæssigt formål.

Informationer klassificeret som andet end Offentlig, skal mærkes med deres klassifikation på papir, i mails, som en del af informationen om afsenderen, og på forsiden af dokumenter hvad enten de er på papir eller i elektronisk form.
Informationer klassificeret som Følsomt, må ikke sendes via ukrypterede mails eller over ukrypterede forbindelser.

1.6 Kommunikationssikkerhed

Brugernes webadgang til internettet scannes i en cloud/proxy-løsning for at tilsikre at der ikke tilgås usikre eller upassende hjemmesider. Adgang til usikre hjemmesider blokeres og filer, der downloades, bliver scannet for virus og andet malware.

Alle indgående e-mails, der modtages i Sentinel Surveillance Systems mailsystem, bliver scannet for usikre links til eksterne hjemmesider og for om det er en potentiel phishing-mail. Derudover scannes vedhæftede filer for virus og andet malware.

Adgang til andre servere/services og Sentinel Surveillance Systems interne netværk sker via VPN beskyttet af 2-faktor autentifikation.

Overførsel af, eller adgang til, Sentinel Surveillance Systems informationer til/fra eksterne samarbejdspartnere eller myndigheder må kun ske efter aftale med disse, baseret på informationernes fortrolighed/klassifikation, herunder om evt. brug af kryptering.

Pc'er og mobile enheder, der kobler sig på virksomhedens netværk og systemer eksternt fra, skal overholde virksomhedens retningslinjer. Dette er kun tilladt for virksomhedens udstyr. Medarbejdernes egne pc'er og mobile enheder (Bring Your Own Device, BYOD) er ikke tilladt på virksomhedens netværk.

1.7 Leverandørstyring og outsourcing

Leverandører, skal overholde Sentinel Surveillance Systems krav til it-sikkerhed.

Der skal foreligge en aftale, og om nødvendigt også en databehandleraftale, som lever op til kravene i databeskyttelsesloven.

Inden indgåelsen af aftalen har Sentinel Surveillance Systems vurderet om der er nogen specielle risici, som aftalen skal tage højde for. Skal personale fra f.eks. rengøringsfirmaet personligt underskrive en fortrolighedserklæring og/eller er der behov for, at de fremviser en straffeattest.

1.8 Medarbejdersikkerhed og awareness

Via awareness-træning sikres, at nye medarbejdere og alle brugere har den nødvendige it-kyndighed, også dem, som ikke har en it-uddannelse, samt en god sikkerhedsadfærd, eksempelvis med hensyn til adgang til

informationer. Dette gælder også, når en medarbejder skifter rolle i virksomheden. Det er den daglige/enkelte leders ansvar, at dette sker.

1.9 Sikkerhedshændelser og it-beredskab

Hvis en medarbejder opdager trusler mod, eller brud på, informationssikkerheden, eller får mistanke om det, skal vedkommende straks underrette ledelsen om dette
Den ansvarlige for den daglige styring af Sentinel Surveillance Systems informationssikkerhed foretager en vurdering af de rapporterede sikkerhedshændelser hurtigst muligt efter at de er anmeldt. Såfremt eksterne parter berøres af sikkerhedshændelser hos Sentinel Surveillance Systems, er den daglige ledelse ansvarlig for eventuel kommunikation over for berørte parter.