Præsentation af Wannafinds sikringsmiljø

Version:	**1.1**
Dato:	**1. marts 2018**

ISO 27001

ISAE 3402 Type 2
Revisorerklæring

Indholdsfortegnelse

Indledning: side 3

Organisering af sikkerhed: side 3

Politikker, procedurer og standarder: side 3

Medarbejdersikkerhed: side 3

Dedikerede sikkerheds- og persondatakompetencer: side 3

Operationel sikkerhed – beskyttelse af kundedata: side 4

Beredskab og disaster recovery: side 4

Håndtering af underleverandører: side 5

Revision, compliance og uafhængige tredjepartsvurderinger: side 5

Indledning

Som hostingleverandør er vores vigtigste sikkerhedsopgave at passe godt på dine data og sørge for, at du til enhver tid lever op til sikkerhedskravene fra dine kunder. Sikkerhed er derfor et område, som vi tager meget seriøst - på alle niveauer.

Formålet med dette dokument er at give dig et indblik i, hvordan vi sikrer vores platform, så du som kunde ikke behøver at bekymre dig om sikkerhed, men i stedet kan bruge tid og energi på at udvikle din forretning.

Organisering af sikkerhed

Vi har etableret et brancheledende informationssikkerhedsprogram (ISMS), der giver vores kunder den bedste beskyttelse og højeste grad af tillid.

Programmet følger ISO 27001-sikkerhedsstandarden, som vi har været certificeret efter siden 2015.

Politikker, procedurer og standarder

Vi har defineret et sæt af politikker, procedurer og standarder for, hvordan vi opererer i virksomheden og bedst passer på dine data. Dokumenterne opdateres løbende, i takt med at trusselsbilledet ændrer sig. På den måde sikrer vi, at vi hele tiden prioriterer vores indsats dér, hvor der er mest brug for den.

Hvordan vi prioriterer indsatsen, afhænger af vores risikovurdering, der opdateres løbende, og som udgør kernen i vores informationssikkerhedsprogram.

Medarbejdersikkerhed

Alle medarbejdere og konsulenter med adgang til systemer og faciliteter er underlagt vores sikkerhedspolitikker. Alle gennemgår obligatorisk undervisning, hvor de bliver præsenteret for alle relevante og aktuelle privacy- og sikkerhedsemner. Dette sker både ved start og løbende gennem deres ansættelse. Formålet er at ruste medarbejderne til at modstå aktuelle trusler mod virksomhedens og kundernes data.

For at højne det generelle niveau i branchen og for at vedligeholde egne kompeencer deltager vores medarbejdere aktivt i communitites og ERFA-grupper. Vi opfordrer vores medarbejdere til hele tiden at være på forkant med den nyeste udvikling og til at erhverve de højeste certificeringer inden for sikkerhed, netværk, osv.

Dedikerede sikkerheds- og persondatakompetencer

Vores sikkerhedschef er ansvarlig for at implementere og vedligeholde vores informationssikkerhedsprogram. Vores interne revisor gennemgår regelmæssigt vores sikkerhedssetup og rapporterer direkte til ledelsen. Endelig har vi interne, juridiske kompetencer inden for persondata, som sikrer, at persondata behandles efter de gældende regler både internt i virksomheden og på vegne af vores kunder.

Beskyttelse af kundedata i flere lag på og flere niveauer

Operationel sikkerhed - Beskyttelse af kundedata

Den vigtigste opgave i vores sikkerhedsprogram er at passe godt på dine data. For at gøre det er vores sikringsmiljø inddelt i flere lag:

- **Fysisk sikkerhed**

Vores datacentre er state-of-the-art og placeret i Danmark. Du kan derfor være sikker på, at dine data bliver inden for landets grænser. Vores datacenterleverandør er ansvarlig for de fysiske rammer som fx strøm, køl, brandslukning og adgangskontrol, og vi fører skarp kontrol med, at vores underleverandører til en hver tid efterlever de gældende sikkerhedsregler på området.

- **Netværk**

Vores netværk er segmentet, så kunder er beskyttet mod hinanden og mod trusler, der bevæger sig på tværs i netværket. Next Generation firewalls begrænser angreb mod kundernes miljøer, og DDoS-beskyttelse begrænser den påvirkning, som evt. angreb måtte have på serverne. Avanceret netværksinspektion opfanger mønstre og angrebsforsøg fra kendte, ondsindede ip-adresser og alarmerer vores driftsafdeling ved behov.

- **Logiske adgange**

Vi tildeler kun rettigheder til de medarbejdere, der har brug for dem, og vurderer dem løbende. Kun særligt privilegerede medarbejdere har adgang til at administrere interne systemer.

- **Overvågning**

Vi overvåger vores infrastruktur og relevante services døgnet rundt. Alle afvigelser registreres i vores incident management-system. Som supplement til overvågningen har vi tilknyttet en 24/7-vagtordning.

- **Logning**

Vi logger alle adgange til management- og kundemiljøer. På den måde sikrer vi integritet og sporbarhed og kan sammenkøre hændelser. Vores centrale logplatform sikrer, at vi hurtigt kan korrelere logs fra mange kilder.

- **Backup**

Vi udfører backup ud fra den indgåede SLA. Backupdata spejles altid mellem to fysisk uafhængige lokationer, så der altid er en tilgængelig kopi i tilfælde af et kritisk nedbrud.

Beredskab og disaster recovery

Beredskab handler om at være forberedt på hændelser, som kan have kritisk eller katastrofal påvirkning på driften. Vi har derfor beredskabsplaner som fastlægger vores procedurer, rutiner og roller i tilfælde af en katastrofe. Medarbejdere trænes i beredskabet flere gange årligt.

For at sikre vores tekniske infrastruktur og sprede risikoen ved kritiske nedbrud bruger vi flere uafhængige datacenterleverandører. Vi opbevarer altid mindst én kopi af backupdata i et datacenter, hvor vi ikke har produktionsdata.

Håndtering af underleverandører

For at vi kan operere så effektivt som muligt, bruger vi underleverandører til udvalgte services. Hvis underleverandørerne kan have påvirkning på vores sikringsmiljø, sørger vi for, at de efterlever samme strenge krav som os selv. Det gør vi via kontrakter, databehandleraftaler, revisionserklæringer, egenkontrol og fortrolighedsaftaler. Vi kontrollerer løbende, at vores underleverandører efterlever kravene.

Revision, compliance og uafhængige tredjepartsvurderinger

Vi har et omfattende compliance-program, som sikrer, at vi efterlever vedtagne standarder, interne politikker og relevant lovgivningen på området, med det formål at understøtte og sikre din forretning:

- **ISO 27001**

ISO 27001 er en international standard for håndtering af informationssikkerhed. Flere af vores konkurrenter påstår, at de følger standarden, men er ikke certificerede. Vi har været certificeret siden marts 2015. Certificeringen skal fornyes én gang om året og revideres af både en intern og ekstern auditør.

- **ISAE 3402 Type 2**

ISAE 3402 Type 2 beskriver, hvordan vi sikrer de ydelser, som vi leverer til vores kunder, og indeholder en uafhængig revisors konklusion på, om beskrivelsen af vores kontroller er retvisende, hensigtsmæssigt udformet, og om kontrollerne har fungeret effektivt i hele erklæringsperioden.

- **BFIH Hostingcertifikatet**

BFIHs Hostingcertikat stiller en række minimumskrav for god hosting, hvad angår kvalitet, stabilitet, gennemsigtighed og kontrol. Hostingcertifikatet læner sig op ad kravene i ISO 27001-standarden, som vi i modsætning til vores nærmeste konkurrenter, har valgt at implementere fuldt ud.

- **PCI DSS 3.2**

Vores betalingskortmiljø har den højeste PCI DSS level 1-certificering, som årligt fornyes efter de strenge krav i PCI DSS-standarden fra VISA og MasterCard.

- **Penetration testing**

Vi udfører regelmæssigt penetration tests mod kritiske komponenter i vores infrastruktur for at se, hvordan vores systemer forsvarer sig mod eksterne trusler.

Kunder kan også udføre penetration tests mod egne systemer efter forudgående aftale med os.