Præsentation af DanDomains sikringsmiljø

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

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 informationssikkerhedsprogram (ISMS), der giver vores kunder den bedste beskyttelse og højeste grad af tillid.

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 sikkerchef er ansvarlig for at implementere og vedligeholde vores informationssikkerhedsprogram. 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.

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 core netværk er redundant, så fysiske nedbrud ikke påvirker normal drift. Firewalls begrænser angreb mod kundernes miljøer, og den påvirkning, som evt. angreb måtte have på serverne. Alle core netværksenheder overvåges, og alarmering sker direkte til 24/7 driftsvagt.

- **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.

- **Backup**

Vi udfører backup ud fra den indgåede SLA. Backupdata flyttes altid til fysisk uafhængig lokation, så der altid er en tilgængelig kopi i tilfælde af et kritisk nedbrud i det primære datacenter.

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.