Sikkerhedspolitik hos ONLINEREGNSKAB A/S

Denne sikkerhedspolitik dækker alle aktiviteter for virksomheden.

Det bestræbes at sikre egne og kunders data med følgende hovedformål:

- Sikre kontinuerlig drift af udbudte tjenester og uhindret adgang til data.
- Sikre at data ikke kan tilgås af udefrakommende eller tredje part uden behørig tilladelse.
- Sikre at data ikke går tabt eller ændres uden klar instruks om dette fra ejer af data.
- Sikre overholdelse af EU's persondataforordning (GDPR) samt anden lovgivning gældende i Danmark.

Ledelse såvel som medarbejdere i virksomheden arbejder løbende med forbedring af sikkerheden. Virksomheden reviderer periodisk om sikkerheden er tilfredsstillende og om tiltag er nødvendige.

Det er ledelsens ansvar at sikre at sikkerhedspolitikken overholdes, revideres løbende og nødvendige tiltag igangsættes.

I tillæg til sikkerhedspolitikken er oprettet interne forretningsgange, som ikke offentliggøres af forretningsmæssige og sikkerhedsmæssige årsager. Vi dokumenterer disse forretningsgange og fører log over kontrol af at disse overholdes med tidspunkt og udfald. Vores kunder og samarbejdspartnere kan kontakte os for uddybning.

Nedenfor er de væsentligste organisatoriske og tekniske virkemidler, som virksomheden benytter til at opnå sikkerheden.

Backup

Vi foretager periodisk backup af data. Dette gælder både kunders og virksomhedens egne data. Hyppigheden, metoden og antal historiske sæt for backup planlægges efter en vurdering foretaget af virksomheden. Her kigges blandt andet på hvor forretningskritiske en gruppe af data er.

Vi kontrollerer jævnligt at backup foretages som planlagt. Dette indbefatter at kontrollere om backup omfatter alle data og at data kan genetableres fuldt ud fra backup.

Der foretages som regel forskellige former for backup af samme data. Det tilstræbes at backupdata findes på flere fysiske lokaliteter og altid vil være

tilgængelig for virksomheden. Produktionsdata og backupdata for disse må ikke udelukkende opbevares hos én og samme underleverandør.

Softwareopdatering

Software og operativsystemer installeret på virksomhedens kontormaskiner og servere holdes opdateret med anbefalede sikkerhedsopdateringer fra de respektive producenter. Vi bestræber os herudover på løbende at opgradere til højeste stabile hovedversion af en given software, så adgang til sikkerhedsopdateringer kan beholdes. Dette sker i det omfang at vores brug, opsætning og egen kode er kompatibel med den nyere version. Hvis dette ikke er tilfældet, vil vi forsøge at opnå dette ved tilpasning og ændringer.

Kontornetværk og arbejdsstationer

Kontornetværket har ikke trådløs adgang (Wifi). Alle kontorets enheder er koblet op med dedikerede kablet forbindelser. Der er oprettet et særskilt trådløst netværk med almindelig internetadgang til brug for gæster og medarbejderes private brug. Kontoret er udstyret med router, som er beregnet til professionel brug af virksomheder. Firewall er opsat således, at alt indgående trafik, som initieres udefra, ikke er tilladt. Adgang til netværket er mulig med VPN for medarbejdere med behov herfor. Her bruges krypteret VPN-forbindelse.

Alle arbejdsstationer har antivirusprogram installeret, som holdes opdateret automatisk. Alle installationer af antivirusprogrammer overvåges med en central tjeneste for om de er aktive og opdaterede. Det er ikke tilladt at installere software på arbejdsstationer til privat brug. Alle medarbejdere skal udvise største omhu og god skik for sikkerhed ved brug af deres arbejdsstation. Det er ikke tilladt at benytte flytbare medier på kontoret, medmindre det er nødvendigt for installation af operativsystem eller der er givet specifik tilladelse af ledelsen.

Alle skærme og tastaturer placeres så de ikke kan aflures udefra og er mest muligt beskyttet mod afluring i øvrigt. Alle enheder og netværksstik kontrolleres jævnligt for om de er blevet udsat for uautoriseret manipulation.

Kontorets arbejdsstationer kræver log ind. Medarbejdere skal altid logge ud fra arbejdsstationer, når de forlader deres plads.

Servere

Alle virksomhedens servere og data er placeret i EU og er direkte administreret af virksomheden. Servere er placeret bag firewall med konservativt opsatte regler, således kun nødvendige porte kan tilgås udefra og fra nødvendige ip-adresser om hensigtsmæssigt. Vi benytter udelukkende udbydere, som har beskyttelse imod ddos angreb.

Medarbejdere

Medarbejdere gøres ved ansættelsens start bekendt med virksomhedens sikkerhedspolitik og informeres ved ændringer. Medarbejder undervises og instrueres i god skik med hensyn til sikkerhed. Medarbejdere opfordres til at komme med forslag, som kan forbedre sikkerheden og er pålagt at indberette alle brud på sikkerhed til ledelsen.

Medarbejdere er underlagt tavshedspligt omkring data og informationer i virksomheden under hele ansættelsestiden og efter endt ansættelse. Medarbejdere må udelukkende bruge deres adgang til data i virksomheden til at udføre opgaver for virksomheden.

Overtrædelse af sikkerhedspolitikken for medarbejdere, kan medføre advarsler og ved særlig grove eller gentagne tilfælde bortvisning med øjeblikkelig inddragelse af alle adgange.

Kunder

Kunder opfordres til at benytte en lang og kryptisk kode ved log ind. Desuden opfordres til ikke at bruge samme kode til flere tjenester samt at skifte kode regelmæssigt. Ved mistanke om at andre har fået adgang til en kode, bør denne ændres hurtigst muligt eller vi kan kontaktes for at spærre adgangen.

Som kunde er man altid velkommen til at kontakte os med eventuelle forslag til forbedring af sikkerheden. Kunder opfordres til at gøre os opmærksom på eventuelle potentielle huller i sikkerheden hos os.

Leverandører

Vi benytter som hovedregel kun leverandører til IT-systemer, som opererer i EU og har dataene placeret i EU. Alle leverandører skal overholde GDPR og vi opretter altid en databehandleraftale. Vi vælger som hovedregel kun leverandører med samme eller bedre sikkerhedsniveau end os selv.

Fysisk sikkerhed

Der er udelukkende adgang til virksomhedens kontor for medarbejdere og eventuelle gæster under ledsagelse af en medarbejder. Kontoret er sikret mod tyveri og brand.

Fysiske dokumenter

Alle dokumenter makuleres (sikker krydsmakulering anvendes) efter brug eller arkiveres i aflåst arkivskab. Kun dokumenter, som er nødvendige at gemme i fysisk form, kommes i arkivskab.

Virksomheden har en "clean desk" politik for alle medarbejdere. Det vil sige at ingen må efterlade dokumenter på kontoret og findes dokumenter skal disse makuleres (sikker krydsmakulering anvendes).

Håndtering af brevpost

Alle modtagne breve behandles hurtigst muligt efter modtagelse. Dette sker ved at de scannes og leveres til den relevante modtager på mail til videre behandling. Herefter makuleres brevene (sikker krydsmakulering anvendes).

Breve til afsendelse med posten eller til levering til modtager direkte, pakkes i konvolut straks efter print. Alle breve som forlader kontoret skal være i forseglet konvolut.

Dataudveksling

Al dataudveksling, som vi foretager på det offentlige internet, sker altid krypteret med højest mulig styrke. Dette gælder også kommunikation på mail.

Intern kommunikation imellem egne systemer, sker som udgangspunkt krypteret, hvis det er muligt og hensigtsmæssigt.

Adgang til tjenester

Ved adgang til vores tjenester skal som minimum benyttes en adgangskode. Vi arbejder desuden for at tilbyde flerfaktor godkendelse ved alle vores log ind.

Ved ændring af adgangskode kræves altid en anden godkendelse. F.eks. adgang til mail eller sms på mobil, som tidligere er tilknyttet til adgangen. I tilfælde af at vi ændrer en kode manuelt for en kunde - f.eks. ved henvendelse på telefon, vil vi først udføre skridt for at sikre, at brugeren reelt er den som må få adgang.

Overvågning

Vi overvåger vores tjenester og servere hele døgnet alle årets dage. Dette gøres med et tredjeparts værktøj, som også opsamler statistik for dokumentation af vores svar tider og oppetid.

Ved nedbrud modtager vi straks underretning herom og vi påbegynder fejlretning straks herefter. Vi melder også ud på vores hjemmesider under driftsstatus, hvis nedbruddet/fejlen har generel og alvorlig påvirkning, som vi vurderer brugere bør blive informeret om. Vi informerer om hændelsens karakter og omfang. Vi opdaterer løbende med fremgang for fejlrettelse og om muligt tidshorisont.

Udover den automatiske overvågning, undersøger vi også henvendelser fra brugere, som kunne tyde på problemer. Vi undersøger også mistænkelige forhold, som vi selv bliver opmærksomme på i vores organisation i dagligdagen.