IT SECURITY POLICY

for

Introdus Onboarding ApS

Oldenborggade 11A.
DK-2300 København S
Denmark

CVR No. 44271028

Updated September 12th, 2023

Content

1. Purpose

Denne IT Security Policy fastlægger rammerne for indførelse, drift og anvendelse af it-systemer, således at Introdus ApS (”Introdus”) til stadighed er en effektiv, pålidelig og troværdig virksomhed.

2. Regulation

Politikken er bl.a. udarbejdet med henblik på at sikre compliance med The General Data Protection Regulation (”GDPR”) (EU) 2016/679 artikel 5, 24, 25 og 32 (Link GDPR).

3. Preamble

Introdus er i stadigt stigende omfang afhængig af, at it-systemer og it-procedurer fungerer effektivt og pålideligt. I revurderingen af denne IT Security Policy indgår konklusionen fra den årlige it-risikovurdering.

4. Objectives

De overordnede målsætninger for denne IT Security Policy er:

- Anskaffelse og anvendelse af it skal understøtte virksomhedens forretningsmæssige aktiviteter og strategier
- Denne IT Security Policy skal omfatte hele it-anvendelsen og sikre, at Introdus til stadighed opfattes som en pålidelig virksomhed, hvor sikring af aktiver har meget høj prioritet

Med udgangspunkt i de overordnede målsætninger skal denne IT Security Policy sikre at:

- it-anvendelsen tilrettelægges med henblik på effektiv udnyttelse af virksomhedens ressourcer.
- it er baseret på hensigtsmæssige hardware- og softwareplatforme
- organisatoriske rammer sikrer et højt it-sikkerhedsniveau
- anskaffelse og anvendelse af it følger en hensigtsmæssig udviklingsplan
- al relevant lovgivning overholdes, eksempelvis persondataloven, ophavsret og bogføringsloven
- it-systemer og tilhørende data har en tilgængelighed, der betyder, at kunderne får den aftalte service, og at virksomhedens funktioner i øvrigt kan udføres uden forretningsmæssige tab
- it-systemer og tilhørende data har en integritet, der sikrer servicekvaliteten, effektiviteten og forhindrer uautoriserede ændringer
- it-systemer sikrer nødvendig fortrolighed omkring data og forhindrer, at data kommer uvedkommende til kendskab
- eventuelle skader som følge af brud på it-sikkerheden begrænses, og at normalisering af forholdene sker inden for en forud fastsat tidshorisont jvf. ”målsætning it-beredskabsplan”.

5. Scope

Denne IT Security Policy gælder for alle aspekter vedrørende specifikation, design, udvikling, test, installation, drift, anvendelse og afvikling af it-systemer, uanset om de udføres af internt eller eksternt personale.

Denne IT Security Policy gælder ligeledes for alle informationssystemer.

5.1 Outsourcing

Såfremt hele eller dele af it-anvendelsen outsources, skal relevante dele af denne IT Security Policy stilles som minimumskrav over for outsourcingleverandøren.

Hvis samarbejdspartnere (kunder, leverandører etc.) får adgang til dele af it-faciliteterne skal disse som minimum efterleve de relevante dele af denne IT Security Policy.

Denne IT Security Policy skal, hvor det er relevant, indgå i aftalegrundlag og kontrakter, som minimum ved henvisning til den til enhver tid gældende IT Security Policy.

Ansvaret for aftale med en evt. outsourcingleverandør påhviler Management. Introdus har i dag, med undtagelse af udvikling, lønsystem og bogførings- og regnskabssystem, ikke outsourcet væsentlige it- systemer.

Enhver beslutning om outsourcing, Cloud og/eller hosting af de primære forretningssystemer (Pre & Onboarding Platform, bogførings- og regnskabssystem) skal godkendes af bestyrelsen.

5.2 Quality Assurance

Kvalitetssikring på it-området skal ske ved:

- at idriftsætning af nye systemer, ændringer til eksisterende systemer og rettelse af fejl sker under kontrollerede former;
- at systemer, data, maskinel og kommunikationsveje beskyttes forsvarligt; og
- at der sker en løbende udvikling, vedligeholdelse og udskiftning af systemer, maskinel og kommunikationsveje

Kvalitetssikringen skal bl.a. opnås ved at der er relevante og betryggende forretningsgange og/eller procedurebeskrivelser for f.eks. brugeroprettelser og opdateringer af forretningssystemer.

Ansvaret for kvalitetssikring påhviler Tech Department.

5.3 Risk Assessment & Contingency Plan

Der skal foreligge en it-risikovurdering der som minimum indeholde afsnit der berører:

- Væsentlige ændringer i it-anvendelsen siden seneste vurdering
- Beskrivelse af de basale it-sikringsforanstaltninger

- Vurdering af risikobilledet på områderne tilgængelighed, datafortrolighed og dataintegritet

Revurdering af it-risikovurderingen skal ske minimum én gang årligt.

Der skal i forbindelse med gennemgang af underleverandører, både årligt og ved overvejelse af nye, laves en risikoanalyse.
Analysen skal vurdere hvilke persondata der indsamles, hvordan det opbevares samt konsekvensen af et eventuelt brud.

Der følges som minimum op på risikovurderingen én gang årligt ifm. den pligtige gennemgang af underleverandører.

Link til Risikovurdering.

Målsætningen for it-risikovurderingen skal godkendes af Board of Directors.

5.4 Contingency Plan

Introdus har ikke en beredskabsplan da omfanget af potentielle risikobrud ikke står mål med indsatsen for at udfærdige, vedligeholde og teste en beredskabsplan.
I stedet beror Introdus sig på best practices indenfor sikkerhed samt daglige backups hvorfra Tech Department vil være i stand til at genskabe funktionalitet og drift hurtigst muligt.

I takt med vækst af virksomheden samt indskærpede krav fra øget data- og kundemængde vil Introdus sørge for at skabe en beredskabsplan når datamængden eller dens sensitivitet kan betragtes som "følsomme oplysninger".

Beredskabsplanen skal indeholde alternative løsninger for virksomhedens drift under et it-nedbrud samt inkludere regler for afprøvning af beredskabsplanen og rapportering heraf.
Opdatering af beredskabsplanen skal ligeledes ske minimum én gang årligt.

Beredskabsplanen godkendes af Management samt Board of Directors.

6. Guidelines

Denne Security Policy konkretiseres i en række retningslinjer opdelt på følgende hovedområder:

- Brugere
- Applikationer
- Platforme og netværk
- Kommunikationsveje
- Fysisk sikring
- Udvikling og idriftsættelse
- Brugeradministration
- Organisation

- Opfølgning på sikkerhedsniveauet
- Klassificering, backup og beredskab.
- Logning

Retningslinjerne er konkretiseret i “Tekniske og organisatoriske sikkerhedsforanstaltninger".

6.1 Procedures

Med afsæt i den ønskede risikoprofil på it-området godkender Board of Directors denne IT Security Policy minimum en gang årligt.

7. Responsibility

7.1 Board of Directors

Med afsæt i den ønskede risikoprofil på it-området godkender Board of Directors denne IT Security Policy minimum en gang årligt.

7.2 Management

Management er ansvarlig for implementering af denne IT Security Policy, herunder uddybning i procedurer, forretningsgange m.v., og for orientering af alle medarbejdere om politikkens indhold.

Management udpeger desuden en Head of IT Security. Head of IT Development er udpeget som Head of IT Security.

7.3 Head of IT Security

Head of IT Security er ansvarlig for at føre tilsyn med overholdelsen af denne IT Security Policy. Head of IT Security skal jævnligt analysere behovet for at justere it-sikkerhedsniveauet samt udarbejde og revidere it-sikkerhedsretningslinjerne.

Det er Head of IT Security’s ansvar, at der er etableret de nødvendige kontroller af sikkerheden, mens berørte medarbejdere er ansvarlige for implementering af kontrolprocedurerne.

7.4 Tech Department

Tech Department står for ajourføring, implementering og vedligeholdelse af it-systemerne og medvirker ved udførelse af sikkerhedsopgaverne.

Tech Department skal registrere eventuelle sikkerhedsbrud i ControlGDPR (Link Data Breach) eller forsøg på samme og regelmæssigt rapportere til Head of IT Security. Head of IT Security drøfter herefter forholdet med Management, medmindre det anses som mindre alvorligt, og forholdet kan herefter afsluttes ud fra Head of IT Security’s anvisninger.

7.5 Users

Brugerne skal efterleve denne IT Security Policy med tilhørende retningslinjer.

Brugerne skal have en tilstrækkelig viden om it-systemerne, så de er i stand til at identificere uregelmæssigheder og være bekendt med konsekvenserne for selskabet, hvis it-sikkerhedsretningslinjerne skulle blive brudt.

Brugerne skal rapportere alle tilfælde af sikkerhedsmæssige brister til Tech Department, som skal registrere henvendelsen og hurtigst muligt derefter informere Head of IT Security.

8. Audit

Såfremt Management vurderer, at det af hensyn til interne forhold i selskabet og/eller kunderelationer vil være nødvendigt med en it-revision eller tilsvarende, kan Management efter godkendelse fra Board of Directors rekvirere en uvildig kontrol, rapport og/eller erklæring som forholder sig til it-sikkerheden.

9. Reporting, Deviation & Dispensation

Head of IT Security skal løbende rapportere til Management om it-sikkerhedsforholdene i virksomheden. Minimum en gang årligt foretages en skriftlig afrapportering om implementeringsgraden af denne IT Security Policy og it-sikkerhedsretningslinjerne.

Såfremt der opstår situationer, som kræver afvigelser fra denne IT Security Policy, skal Management skriftligt anmodes om dispensation. Anmodningen skal indeholde en risikovurdering og tilstrækkelig dokumentation for alle risici.

9.1 Involvement of Board of Directors

Ved brud på denne IT Security Policy, der bevirker eller med stor sandsynlighed ville bevirke, at Introdus enten ikke er funktionsdygtig på flere betydende funktioner eller datafortroligheden brydes, skal Head of Security orientere bestyrelsen snarest herom.

10. Separation of Duties

Der skelnes i it-området mellem it-udvikling og it-drift.

I Introdus foretages der intern it-udvikling af Pre & Onboarding Platformen.

Alle væsentlige systemer, som benyttes i it-udviklingen som [Atlassian Software Suite (Bitbucket, Jira, Confluence)] er købt, videreudvikles og vedligeholdes eksternt.

Tech Department ledes af Head of Development. Tech Department har udover udvikling af Pre & Onboarding Platformen til opgave at samle og systematisere virksomhedens data samt at foretage rapportering samt håndtere it-drift af it-infrastruktur og support af virksomhedens brugere og kunder.

Tech Department er som led i funktionsadskillelse ikke involveret i den forretningsmæssige drift udover support af kunderne. Dette er der taget højde for i indretningen af de anvendte it-systemer

og ved de tildelte brugeradgange. Hvis der opstår en situation, hvor adskillelsen ikke kan opretholdes, skal der implementeres kompenserende tiltag efter en forudgående godkendelse fra Management.

11. Separation between Development, Testing & Operation

Det skal sikres, at der er adskillelse mellem udvikling, test og driftsmiljøer.

For de primære forretningssystemer skal som minimum gælde:

- Der skal være skriftlige godkendte vejledninger for opgraderinger/ændringer af livemiljø, og opgraderinger/ændringer skal implementeres på betryggende vis
- Udvikling-og eller testmiljøer skal være teknisk adskilte fra livemiljø, og det skal tilstræbes at testmiljøer er så identiske med livemiljøet som muligt

12. Independence of Key Employees

Introdus skal tilstræbe uafhængighed af enkeltpersoner gennem etablering af personbackup eller anden backup for de medarbejdere, der er alene om at dække specialer eller systemer af væsentlig værdi for virksomheden.

Dokumentation specielt hørende til sådanne områder skal løbende ajourføres. Eksempel på dokumentation kan være:

- Systemdokumentation
- Indtastningsvejledninger
- Dokumentation af slutbrugerværktøjer
- Forretningsgange m.m.

13. Approval

The IT Security Policy has been approved by the Board of Directors at the Board Meeting held on 5 August 2021.