info@business-institute.dk
Telefon: 98 18 80 00

IT sikkerhedspolitik for Business Institute A/S

Indholdsfortegnelse

info@business-institute.dk
Telefon: 98 18 80 00

Offentlig sikkerhedspolitik for Business Institute

1. ANVENDELSESOMRÅDE

Denne politik udgør de overordnede rammer for informationssikkerheden i virksomheden, både i virksomheden som selskab og i alle virksomhedens leverancer til kunder.

INDLEDNING OG FORMÅL

Formålet med informationssikkerhed i virksomheden er at:

- Beskytte fortrolighed, integritet og tilgængelighed af information og informationssystemer. Med dette forstås:
  - **Fortrolighed** – sikkerhed for, at adgang til informationer kun gives til de personer, som har godkendt adgang hertil.
  - **Integritet** – sikkerhed for, at information er korrekt og ikke på nogen måde er blevet ændret eller manipuleret, hvad enten dette er utilsigtet eller med forsæt.
  - **Tilgængelighed** – sikkerhed for, at informationer og informationssystemer er tilgængelige inden for de fastsatte rammer og aftaler.
- Sikre at virksomheden til enhver tid lever op til gældende lovgivning og regulativer samt kontraktuelle krav.
- Virksomheden arbejder med informationssikkerhed for at underbygge virksomhedens forretningsmodeller, finansielle resultater, samt virksomhedens troværdighed over for omverdenen, herunder samarbejdspartnere, kunder og myndigheder.
- Virksomheden tilsikrer, at tekniske eller procedurebaserede kontroller, der implementeres i virksomheden, sker på baggrund af en effektiv risikovurdering.
- Opretholde virksomhedens omdømme som en sikker og troværdig leverandør.

ROLLER OG ANSVARSOMRÅDER

Følgende roller og ansvar er defineret:

Rolle	Ansvar
Ledelse	Ledelsen i virksomheden har ansvar for at sætte retningslinjer for, og overholdelse af lovgivningen omkring persondata
Medarbejdere	Skal i deres daglige arbejde efterleve de politikker og procedurer, som virksomheden har udfærdiget omkring behandling af persondata.

RAMMER OG GYLDIGHED

Informationssikkerhedspolitikken skal finde anvendelse for:

A. Enhver information virksomheden ejer, kan gøres ansvarlig for, eller behandler, uanset hvilken form denne opbevares eller formidles i. Dette gælder uafhængigt af hvilken teknologisk platform, der anvendes til opbevaring og behandling.
B. Alle virksomhedens medarbejdere, midlertidige medarbejdere, samarbejdspartnere og konsulenter, serviceleverandører, underleverandører og deres medarbejdere.

info@business-institute.dk
Telefon: 98 18 80 00

C. I alle outsourcing-forhold, hvor der anvendes eller tildeles adgang til virksomhedens informationer og systemer.

COMPLIANCE

Virksomhedens ledelse forpligter sig til at tilsikre løbende forbedring af ledelsessystemet for informationssikkerhed.

VIRKSOMHEDENS SIKKERHEDSPRINCIPPER

Virksomhedens virke afhænger i høj grad af sikker håndtering af informationer i både elektronisk og fysisk form. Af denne grund er informationssikkerhed en integreret del af virksomhedens forretningssikkerhed.

Sikkerhed er en del af virksomhedens DNA.

VEDLIGEHOLDELSE AF KOMPETENCER

Virksomheden vedligeholder, understøtter og fastholder vidensniveauet hos alle medarbejdere for at understøtte sikker behandling af informationer i virksomhedens informationssystemer. Dette foregår ved inkludering af virksomhedens forretningsenheder i relevante fora samt løbende uddannelse af virksomhedens medarbejdere.

TROVÆRDIGHED

Såfremt eksterne parter berøres af sikkerhedshændelser hos virksomheden, vil virksomheden kommunikere ærligt og troværdigt over for berørte parter.

2. DETEKTERING OG HÅNDTERING AF SIKKERHEDSHÆNDELSER

Virksomheden har etableret en proces til håndtering af sikkerhedshændelser med det formål at sikre, at virksomheden reagerer hensigtsmæssigt på faktiske eller formodede sikkerhedshændelser vedrørende informationssystemer og data. Eksempler på sådanne sikkerhedshændelser kan være ulovlig indtrængen, kompromittering af systemer, misbrug af oplysninger og informationsressourcer og brud på kontinuitet af kritiske informationssystemer og processer.

3. KLASIFICERING AF DATA

IT-afdelingen klassificerer behandlede data og oplysninger inden for forretningen eller støtteprocesser og tilpasser disse til de underliggende applikationer og systemer for at dække forretningens sikkerhedsmæssige krav til tilgængelighed, fortrolighed og integritet.

De klassificering niveauer, der anvendes hos virksomheden er:

- Fortroligt (herunder persondata)
- Intern
- Offentligt

Til dette formål bruger virksomheden en struktureret tilgang til at identificere de forretningsmæssige krav og for at vurdere de potentielle trusler om databehandling hos virksomheden

4. ADGANGSKONTROL

Adgang til ressourcer og applikationer godkendes af den respektive systemejer, som hos Business Institute A/S er ledelsen. Der foretages halvårlige recertificering af brugernes adgang til de respektive systemer. Dette udføres af ledelsen hos Business Institute A/S.

Uautoriseret adgang:
Brugere af virksomheden informationsressourcer skal afstå fra at forsøge at opnå eller tillade andre at opnå uautoriseret adgang til systemerne. Det er brugerens pligt at indberette enhver afvigelse fra de politikker og procedurer til den ansvarlige.

Fjernadgang:
Fjernadgang til virksomhedens IT-infrastruktur udefra må kun forsøges ved hjælp af bærbare faciliteter, som virksomheden leverer. Adgang fra internet til SuperOffice, administrativ og produktionsnet beskyttes med to-trins godkendelse såfremt man er bevilliget fjernadgang. Adgang til Umbraco må kun ske fra arbejdsstationerne ved BI, eller en BI krypteret labtop.

Brugertildelt brugernavn og password:
Brugere kan kun få adgang til computersystem ved hjælp af autoriseret brugernavn og adgangskode. Brugere må ikke anvende andre brugernavne eller adgangskoder for at få adgang til virksomhedens computersystemer end deres egne. Desuden skal brugerne ikke bevidst tillade brugen af deres brugernavn og adgangskode af andre, uanset om en sådan person er en autoriseret bruger eller ej. Brugerne er også gjort opmærksom på, at de er ansvarlige for alt arbejde, gemt eller hentet, meddelelser, der sendes eller modtages, eller transaktioner, som udføres via internettet under deres brugernavn og adgangskode, hvis foranstaltninger for at beskytte fortroligheden af disse legitimationsoplysninger ikke er taget. Brugerens brugernavn og adgangskode må ikke genbruges til andre internet tjenester så LinkedIn, Facebook eller lign. Der roteres ikke password, men brugerne genereres selv et password på minimum 8 karakterer. System password gemmes i en password manager. Systemerne risikovurderes og ved ophør af medarbejdere med adgang til forretningskritiske systemer, skiftes password på disse.

Adgang til uautoriserede netværk/services:
Brugere må ikke få adgang til eller forsøge at få adgang til netværk, netværksdrev og aktiver og mapper, for hvilke brugeren ikke har nogen legitim grund til adgang, uanset om brugeren har ret til at gøre det eller ej (need-to-know).

5. BEREDSKABSPLAN

Virksomheden har etableret en beredskabsplan, som tilsikrer, at virksomhedens forretningsprocesser er beskyttede mod effekten af større fejl i informationssystemer og katastrofer, og som tilsikrer en rettidig genskabelse af de ramte services og beskyttelse af Virksomhedens medarbejdere.

6. LEVERANDØR STYRING

Virksomheden skal opretholde passende niveauer af informationssikkerhed og service levering i overensstemmelse med aftaler med tredjepart.
Levering af tjenester:
Tjenesten leveret af tredjemand bør omfatte sikkerhedsforanstaltninger, service definitioner og af service management aftalte.
Overvågning og revision af tredjeparts-tjenester:

Tredjepartstjenester, rapporter og optegnelser skal overvåges og gennemgås regelmæssigt.

Der indhentes databehandler aftale med leverandørerne. Samtidig laves der hvert år en audit af databehandlerne.

I praksis vil dette foregå ved at indhente 3. part revisionserklæring fra leverandørerne.

7. SYSTEM UDVIKLING OG VEDLIGEHOLDELSE

Testmiljøer skal holdes enten fysisk eller logisk adskilt fra produktionsmiljøer. Testmiljøer til applikationer skal som udgangspunkt opfylde de samme sikkerhedskrav, som produktionssystemer, især hvis der anvendes produktionsdata til testformål. Det er projektlederens ansvar at opfylde denne regel.

Efter et nyt system er blevet placeret i drift, skal alle program- og procedure ændringer godkendes før gennemførelsen for at afgøre, om de er blevet godkendt, testet og dokumenteret.

Operationel og supportepersonale skal have relevant uddannelse, så de kan køre det nye system på en sikker måde. Alle nye systemer skal have passende drifts- og support dokumentation.

Der udføres change management på alle udviklingsopgaver.
Privacy by design og privacy by default tænkes ind i udvikling af applikationer/services.

8. BRUGER TRÆNING

Alle virksomhedens medarbejderes bevidsthed om it-sikkerheds relaterede emner skal styrkes med jævne mellemrum. Uddannelse og information er vigtige for it-sikkerhed og en sikkerhedsdrevet adfærd af slutbrugeren. **Bestyrelsen/direktionen bestemmer**, hvilken uddannelse er passende for dets personale med adgang til fortrolige oplysninger ved at overveje risikoen og derefter afbalancerer omkostningerne ved sikkerhedsforanstaltningerne mod risikoen.

9. OVERTRÆDELSE AF VIRKSOMHEDENS SIKKERHEDSREGLER

Overtrædelser af virksomhedens sikkerhedsregler vil kunne medføre sanktioner over for medarbejdere i overensstemmelse med virksomhedens personalepolitik. Over for samarbejdspartnere, leverandører og deres medarbejdere vil sanktionen kunne ske i overensstemmelse med indgåede aftaler.

10. OPFØLGNING OG GODKENDELSE

Denne sikkerhedspolitik revurderes én gang årligt eller ved større ændringer i det overordnede risikobillede, i virksomhedens overordnede forretningsstrategi eller i organisationen.

Denne politik er godkendt og revideres af ledelsen.

info@business-institute.dk
Telefon: 98 18 80 00

11. DOKUMENTINFORMATION

Dokumentinformation:

Kritikalitet: Offentlig

Dokumentforfatter: direktør Lars Ib

Dokumentansvarlig: direktør Lars Ib

Godkendt af: bestyrelsesformand Jan Holmsgaard

Version	Ikrafttrædelses-dato	Tekst / ændringer	Hvem	Dokumentnavn
1.0	23.04.2018	Nyt dokument.	Lars Ib	IT-Sikkerhedspolitik 1.0.docx