BEMIIT

Bemiit ApS
IT-sikkerhedspolitik

BEMIIT

Dokument information

Virksomhed	Bemiit
Titel	Bemiit IT-sikkerhedspolitik
Forfatter	Bent Brix Pedersen
Dokument ejer	Bent Brix Pedersen

Revisions historik

Revisions dato	Version nummer	Revideret af	Revisions beskrivelse
Jan-2023	3	Bent Brix	Dokument oprettet

BEMIIT

Indhold

BEMIIT

1 Introduktion

Bemiit er en virksomhed der har specialiseret sig i at udvikle, drifte og supportere en kommunikationsplatform til bl.a. grafiske produkter, hvor Bemiit benytter ejet udviklet software. Bemiit har oparbejdet viden og kompetencer i at arbejde med teknologier som er relevante for en sådan handels- og kommunikationsplatform.

Der behandles mange forskellige informationer såsom arbejdsrelateret, personlige og kan også være personfølsomme informationer indenfor for de implementerede informationssystemer i Bemiit. Sikkerheden er derfor et vigtigt område for Bemiit således dennes kunder, interessenter og samarbejdspartnere kan være sikre på at deres informationer bliver behandlet sikkerhedsmæssigt forsvarligt.

BEMIIT' IT-sikkerhedspolitik udmøntes i praksis ved en IT-driftsvejledning, hvori interne IT-sikkerhedsprocedurer og specifikationer for IT-sikkerheden i Bemiit er beskrevet i bilag 2 IT-driftsvejledning. Derudover udmøntes den ved de IT-sikkerhedsforanstaltninger der er fastsat ved Amazon Web Services center, Stockholm SE, ved nærmere information kontakt Bemiit eller se bilag Amazone.

2 Formål

Bemiit har en IT-sikkerhedspolitik hvor alle informationer der er i forretningens besiddelse beskyttes med et højt fokus på fortrolighed, integritet og tilgængelighed, som tilstræbes, opretholdt til alle tider.

Derfor er formålet med dette dokument at beskrive BEMIIT' IT-sikkerhedspolitik således at vi over for interessenter, samarbejdspartnere og kunder kan dokumentere at Bemiit arbejder forsvarligt med beskyttelsen af informationer.

3 Omfang

Retningslinjerne nævnt i denne IT-sikkerhedspolitik gælder for alle systemer, mennesker og forretningsprocesser der udgør forretningssystemet Bemiit. Dette inkluderer ledelsen, medarbejdere og kontrakt bundne eksterne partnere som har adgang til informationssystemer eller information anvendt til BEMIIT' formål.

4 Definitioner

Denne IT-sikkerhedspolitik bør gælde når BEMIIT' informationssystemer bliver anvendt. Information kan tage mange former hvilket inkluderer, men er ikke begrænset til, følgende:

- Fysiske eksemplarer med data printet eller skrevet på papir.
- Data gemt elektronisk.
- Kommunikation sendt med post, hvad end det er budbringer eller elektronisk.
- Gemt lyd eller video.

5 Sikkerhedsniveau

Formålet med dette afsnit er at angive hvilke instanser der har indflydelse på BEMIIT' informationssystemer.

IT-sikkerhedspolitikken søger at tilgodese de anerkendte standarder for informationssikkerhed og tilstræbes at gennemgå årlig IT Sikkerhedstjek af ekstern 3. parts af IT-rådgivninger.

6 Rolle- og ansvarsfordeling

Formålet med dette afsnit er at beskrive rolle- og ansvarsfordelingen der er etableret i Bemiit.

Ledelsen har det overordnede ansvar for IT-sikkerheden, herunder ansvaret for overholdelse af de nævnte retningslinjer, samt uddelegering af ansvarsområder blandt en række medarbejdere.

- IT-chefen er ansvarlig for risikovurderinger samt fremtidige revurderinger af IT-sikkerhedspolitikken.
- Udviklingschefen har det daglige ansvar for kritiske processer indbefattet i BEMIIT' informationssystemer.
- Ledelsen har ansvaret for at IT-sikkerhedspolitikken godkendes en gang årligt.

7 Klassifikation af informationssystemer

Formålet med en klar klassifikation af de informationssystemer Bemiit vælger at implementere er at det hjælper til at sikrer at det implementerede har relevans, det implementeres ud fra risiko og at det understøtter forretningen i sin helhed.

Alle informationssystemer der udvikles og arbejdes med i Bemiit tilstræber at overholde gængse standarder fastsat for IT Sikkerhed, hvorfor kravene til informationssystemer i Bemiit søger:

- Fortrolighed: Informationssystemer i Bemiit skal beskyttes mod uautoriseret adgang og misbrug.
- Integritet: Informationssystemer i Bemiit skal være komplette, præcise og beskyttet mod misbrug, samt at systemerne fungerer efter hensigten.
- Tilgængelighed: Informationssystemer er til en hver tid tilgængelig på de tidspunkter som er påkrævet.

For yderligere information om hvordan BEMIIT' informationssystemer sikres i praksis, henvises til bilag 2, IT-driftsvejledning. Fremsendes på opfordring og efter behov.

8 Risiko områder

8.1 Personalets ansvar

Formålet med dette afsnit er at beskrive retningslinjerne for personalet angående informationssikkerhed.

- Medarbejdere må under ingen omstændigheder udtrække personfølsomme oplysninger ud af BEMIIT' informationssystemer.
- Medarbejdere med adgang til personfølsomme oplysninger skal underskrive en tavshedserklæring.
- Medarbejdere med adgang til Bemiit informationssystemer har gennemgået et uddannelsesforløb i sikker brug af IT-systemer og data herunder internet og e-post.
- Relevante medarbejdere er bekendt med procedurer for rapportering af sikkerhedsproblemer og brud på IT-sikkerheden.
- Relevante medarbejdere skal informeres om at deres aktivitet overvåges og logges.

8.2 Fysisk IT-sikkerhed

Formålet med dette afsnit er at beskrive retningslinjerne for fysisk IT-sikkerhed.

- IT-udstyr og backup skal til en hver tid beskyttes mod skader forårsaget af fysiske årsager som tyveri, hærværk, vand, brand og røg.
- Kritisk IT-udstyr som servere og andre netværkskomponenter skal opbevares på lokaliteter med begrænset adgang.
- Ikke kritisk udstyr bør ikke placeres på lokaliteter uden opsyn.
- Der skal tages relevante forholdsregler i forhold til forsyningssvigt.
- IT-udstyr og data som befinder sig udenfor BEMIIT' lokaliteter, herunder arbejdspladser og mobilt udstyr, skal af de personer der har fået overdraget udstyret, sikre det overfor uautoriseret adgang og misbrug.

8.3 Data kommunikation

Formålet med dette afsnit er at beskrive de fastlagte sikkerhedsretningslinjer der er gældende for datakommunikation i BEMIIT' informationssystemer.

- Medarbejdere I Bemiit skal som udgangspunkt kun have adgang til de system relevante områder der skal til for at de kan udføre deres arbejdsopgaver.
- Data skal som udgangspunkt lagres på centralt IT-udstyr, såsom servere.
- Der skal foretages backup af data således at dette kan gendannes med mindst muligt tab samt skal data gemmes på flere lokationer.
- Data omhandlende personfølsomme oplysninger er forbudt at kopiere samt medbringe udenfor BEMIIT' informationssystemer, andet data skal behandles med forsigtighed.
- Brugen af udadgående kommunikation såsom e-mail skal som udgangspunkt foregå til arbejdsrelateret opgaver men dog lovligt til private anliggender med sund fornuft.

8.4 Kontrol og overvågning

Formålet med dette afsnit er at beskrive hvordan Bemiit sikrer autoriseret adgang og overvågning af deres informationssystemer.

- BEMIIT' informationssystemer skal beskyttes mod uautoriseret adgang og adgang til systemerne skal foregå ud fra et princip om at det skal være arbejdsrelateret.
- Adgang til BEMIIT' informationssystemer skal foregå ved brugen af passwords der søger at opfylde kompleksheds kravene udstukket af Microsoft.

- Der foretages stikprøvekontroller af de implementerede sikkerhedsredskaber for at sikre konstant overholdelse af retningslinjerne.

9 Brud på IT-sikkerhedspolitikken

Overtrædelse af IT-sikkerhedspolitikken der findes af væsentlig karakter, vil blive anset som en misligholdelse af ansættelsesforholdet, hvilket kan medføre advarsel, opsigelse, bortvisning eller erstatningskrav.