Ad-Hoc Projekt

§§ 43, 85, 107, 108, 110 TILBUD

IT & E-mailpolitik

AD-HOC PROJEKT | VESTERGADE 9, 6520 TOFTLUND

Ad-Hoc Projekt
En socialfaglig indsats

Indholdsfortegnelse

IT & E-mailpolitik

Indledning

Ad-Hoc Projekts IT-politik har til formål at beskytte og sikre virksomhedens data og systemer, herunder personoplysninger. Politikken bidrager til at beskytte Ad-Hoc Projekts værdier og omdømme og gælder for alle virksomhedens medarbejdere.

For at sikre videndeling i virksomheden og for at sikre bedst mulig kommunikation skal alle medarbejdere anvende de informationssystemer, som Ad-Hoc Projekt stiller til rådighed efter Ad-Hoc Projekts anvisning.

Password

- Password = Mindst 8 tegn (min. et stort bogstav, et lille bogstav og et tal)
- Password er personligt og må under ingen omstændigheder udleveres til andre
- Password skal skiftes hver 12 måned (systemet beder om nyt password automatisk)
- Passwords kan ikke genbruges

Ad-Hoc Projekt ApS – Vestergade 9, 6520 Toftlund
Tlf: 7735 5000 – Mail: Kontakt@ad-hoc-projekt.dk – CVR-nummer: 4384 3230

- Hvis kontoen er låst (fejl ved login fx tre forkerte indtastninger), åbnes kontoen efter 30 min. Inden for arbejdstid kan du ringe til IT-afdelingen på 7735 5000 for at få genåbnet din konto

Adgang til systemer, programmer og information

Du må ikke uden tilladelse:

- Tilgå eller kopiere data fra systemer eller programmer, som du ikke har autoriseret adgang til
- Bruge programmer/software uden at have betalt for retten til at anvende dem
- Købe programmer til brug i Ad-Hoc Projekt

Ad-Hoc Projekt benytter kun ægte og licenserede programmer.

Backup/sikkerhedskopiering

- IT-afdelingen sikrer, at der tages backup af data på alle netværksdrev, e-mails og systemer
- Den enkelte medarbejder er ansvarlig for at tage backup af data, der gemmes på eksterne drev, fx USB-stik, mobiltelefon, tablet eller på lokalt drev på computer
- Hvis IT-afdelingen vurderer, at arbejdsredskabet skal reinstalleres, sker det uden hensyntagen til data gemt lokalt

Fysisk og elektronisk sikkerhed

Alle medarbejdere er ansvarlige for sikkerheden på arbejdspladsen og skal derfor følge nedenstående regler:

- Når du forlader arbejdspladsen efter endt arbejdstid, skal du sikre, at vinduer er lukkede, døre låst og alarmen er sat til
- Bærbare computere skal lægges i aflåst skuffe, skab eller kontor eller tages med hjem
- Computeren skal slukkes, når du går hjem
- Computeren skal låses, når du forlader din plads
- Hvis Ad-Hoc Projekts systemer tilgås fra ekstern computer, skal medarbejderen huske at logge af virksomhedens systemer og lukke browser ned efter brug mv.
- Der skal være lås eller kode på alle mobiltelefoner, som synkroniserer e-mail/kalender, da disse data ellers ligger helt frit, hvis du mister mobiltelefonen
- På virksomhedens mobiltelefoner og computere skal der være skærmlås og automatisk logoff.

Internet

Internettet skal ses som et hjælpemiddel og en vigtig informationskilde til løsning af dine daglige arbejdsopgaver. Følgende regler gælder for brug af internettet:

Ad-Hoc Projekt ApS – Vestergade 9, 6520 Toftlund
Tlf: 7735 5000 – Mail: Kontakt@ad-hoc-projekt.dk – CVR-nummer: 4384 3230

- Ad-Hoc Projekt forudsætter, at brug af internettet ikke medfører en forringet arbejdsindsats, og at du agerer loyalt overfor Ad-Hoc Projekt ved brug af internettet
- Internetadgangen må kun benyttes til søgninger, der ikke strider mod almindelige etiske standarder. Særligt må internetadgangen ikke benyttes til adgang til pornografiske websites eller websites, der er af politisk/religiøst, voldeligt/stødende, ekstremistisk eller diskriminerende karakter. Det er ligeledes i strid med Ad-Hoc Projekts politik at viderebringe materiale med et sådant indhold
- Det er ikke tilladt at besøge websites, som udløser betalingsforpligtelser for Ad-Hoc Projekt
- Du må ikke downloade programmer fra internettet, medmindre der er truffet særskilt aftale med IT-afdelingen/den IT-ansvarlige herom.

E-mails samt øvrige kommunikationsplatforme

- E-mails og øvrige kommunikationsplatforme mv. (fx Teams) er arbejdsredskaber
- *Ikke-arbejdsmæssig anvendelse af e-mails skal begrænses mest muligt og må ikke belaste arbejdstiden eller påvirke arbejdsindsatsen i negativ retning*
- Alle e-mails mv. afsendt og modtaget på Ad-Hoc Projekts systemer anses som Ad-Hoc Projekts ejendom
- Du må ikke sende e-mails mv., der indeholder pornografisk, voldeligt/stødende, politisk/religiøst, ekstremistisk eller diskriminerende materiale, og indhold af e-mails skal afspejle gensidig respekt og høflighed
- Informationer, der har relevans for alle medarbejdere, skal publiceres på intranettet. Undgå at sende ”alle-e-mails”
- Indhold med følsomme oplysninger og oplysninger af fortrolig karakter skal sendes via krypteret e-mail
- Hvis der benyttes formularer fra websites, hvor følsomme personoplysninger og personnummer kan indtastes og fremsendes, skal der anvendes kryptering.
- E-mails slettes automatisk fra Outlook efter 5 år

Virus og spam

For at undgå hackerangreb, systemnedbrud og lignende skal du overholde følgende:

- Brug sund fornuft og dømmekraft inden du åbner e-mails fra ukendte afsendere
- Åbn ikke vedhæftede filer af ukendt karakter
- Klik ikke på links i e-mails fra fx ”Skat” eller din bank uden først at have tjekket, at linket fører hen til en troværdig website. Ved at holde musen hen over linket, vises adressen nederst til venstre
- Benyt knappen ”Uønsket mail” i Outlook for at rydde op i spam
- Undlad at videresende masse-e-mails om virus- eller spamadvarsler, da disse ofte er spam/virus i sig selv. Kontakt i stedet IT-afdelingen
- Det er ikke tilladt at anvende USB-stik/Du må kun anvende USB-stik, som er godkendt af IT-afdelingen
- Har du mistanke om, at din pc mv. er angrebet af virus, skal du omgående kontakte IT-afdelingen

Ad-Hoc Projekt ApS – Vestergade 9, 6520 Toftlund
Tlf: 7735 5000 – Mail: Kontakt@ad-hoc-projekt.dk – CVR-nummer: 4384 3230

- Virksomheden skal sikre den nødvendige fortrolighed, integritet, tilgængelighed og robusthed af IT-systemer mv. Det betyder bl.a., at der sker løbende ajourføring af servere og pc-arbejdspladser med sikkerhedsopdateringer af software mv., og at computere skal have en opdateret firewall og et antivirusprogram installeret, som lever op til passende sikkerhedsmæssige standarder.

E-mails m.v. i forbindelse med fratrædelse

- Det er dit ansvar, at private e-mails, Teams-beskeder mv. bliver slettet i forbindelse med ansættelsesforholdets ophør
- Private meddelelser, der ikke er slettet ved ansættelsesforholdets ophør, bliver slettet af Ad-Hoc Projekt
- Det er dit ansvar at overdrage forretningsrelevante dokumenter og e-mails til nærmeste leder og informere om møder, der er aftalt med kunder mv.
- Ad-Hoc Projekt beslutter, hvornår din e-mailkonto og evt. andre kommunikationsplatforme bliver lukket. Konti lukkes dog senest 12 måneder efter fratrædelse
- Meddelelser, der modtages efter ansættelsesforholdets ophør og indtil lukning af din e-mailkonto mv., kan blive åbnet af Ad-Hoc Projekt. Kun få betroede medarbejdere vil have adgang
- Private meddelelser, herunder e-mails, der er markeret som ”privat”, ”personligt” eller på anden måde er angivet til at have et privat indhold, vil ikke blive åbnet
- Efter din e-mailkonto mv. er lukket, vil al post sendt til den pågældende konto tilgå Ad-Hoc Projekts administratorkonto
- Snarest muligt efter at du har forladt arbejdspladsen, og du ikke længere har adgang til e-mailkontoen mv., indsætter Ad-Hoc Projekt et autosvar med oplysning om, at du er fratrådt samt eventuel anden relevant information
- Indtil e-mailkontoen mv. er lukket, bliver den alene benyttet til modtagelse af meddelelser
- Oplysninger om e-mailadresse og øvrige kontaktoplysninger bliver hurtigst muligt fjernet fra Ad-Hoc Projekts website og andre offentligt tilgængelige informationssteder
- Både arbejdsrelaterede og private e-mails bliver ikke videresendt, og modtager får et autosvar om, at medarbejderen er fratrådt.

Ad-Hoc Projekts adgang til e-mailpostkasser mv. og logning af internetbrug

- Af drifts- og sikkerhedsmæssige hensyn registrerer virksomheden brug af internettet og e-mails. Bl.a. for at opnå den tilstrækkelige sikkerhed i forbindelse med virksomhedens behandling af personoplysninger har virksomheden i den forbindelse foranstaltninger til sikring af, at det efterfølgende er muligt at undersøge og fastslå om og af hvem, der har behandlet personoplysninger, herunder ved logning. Med henblik på sikring af virksomhedens fortrolige og forretningskritiske oplysninger har virksomheden tillige foranstaltninger til sikring af, at det efterfølgende er muligt at undersøge og fastslå om og af hvem, der har behandlet fortrolige og forretningskritiske oplysninger, herunder ved logning
- Ad-Hoc Projekt udfører ikke systematisk kontrol og overvågning af medarbejdernes e-mails, herunder andre kommunikationsplatforme, fx Teams og internetbrug mv. En målrettet

Ad-Hoc Projekt ApS – Vestergade 9, 6520 Toftlund
Tlf: 7735 5000 – Mail: Kontakt@ad-hoc-projekt.dk – CVR-nummer: 4384 3230

stikprøvekontrol eller overvågning af en enkelt medarbejders anvendelse af e-mails, internet mv. vil derfor som udgangspunkt ikke finde sted [1]
- Ved konkret mistanke om misbrug mv. i strid med virksomhedens retningslinjer eller interesser kan kontrol og/eller overvågning af en enkelt medarbejders anvendelse af e-mails og internet mv. dog blive aktuel
- I tilfælde af kontrol eller overvågning vil medarbejderen efterfølgende blive informeret om baggrunden herfor, hvem der har deltaget samt om resultatet og konsekvenserne heraf. Kontrol og overvågning vil blive foretaget af den IT-ansvarlige som begge vil være underlagt tavshedspligt

Intranet

- Alle relevante informationer vedrørende IT-sikkerhed publiceres på intranettet
- Medarbejderne har ansvaret for at holde sig opdateret på publiceret information

Mobiltelefoner

- Der skal være lås på alle mobiltelefoner, jf. afsnittet om "Sikkerhed"
- Forud for indkøb/bestilling af en mobiltelefon skal din leder godkende købet
- Når du stopper i Ad-Hoc Projekt, skal mobiltelefonen afleveres i IT-afdelingen. Du er selv ansvarlig for at tage backup af og slette alt privat indhold på mobiltelefonen
- Mister du din mobiltelefon, skal du kontakte Telenor på tlf. nr. 71 120 000 for at få spærret simkortet

Det er ikke tilladt at bruge private enheder mv. som arbejdsredskab. Det er herunder ikke tilladt at behandle eller gemme Ad-Hoc Projekts fortrolige og følsomme oplysninger på udstyr, der ikke tilhører virksomheden. Du må heller ikke bearbejde modtagne filer eller downloade virksomhedens dokumenter eller e-mails mv. til din private PC, Dropbox, cloudløsning, private e-mailkonto, såsom Gmail etc.

Brud på datasikkerheden

Du skal rapportere til IT-afdelingen om sikkerhedshændelser, der kan påvirke eller formodes at ville påvirke virksomhedens informationer.
Hvis du bliver opmærksom på, at der er sket et databrud, skal der tages hånd om det snarest og inden for 72 timer. Du skal derfor med det samme kontakte Bo Højlund Christensen som vil vurdere, om sagen skal meldes som et databrud til Datatilsynet.

Eksempler på databrud:

- Mistet PC
- Mistet telefon, USB-stik eller iPad med Ad-Hoc Projekts data på
- E-mail/data sendt til forkert modtager

[1] Hvis der i stedet for indføres egentlig stikprøvekontrol fremfor kun ved konkret mistanke, orienteres medarbejderne herom.

Ad-Hoc Projekt ApS – Vestergade 9, 6520 Toftlund
Tlf: 7735 5000 – Mail: Kontakt@ad-hoc-projekt.dk – CVR-nummer: 4384 3230

- Data er blevet gjort offentligt tilgængeligt ved en fejl
- Mistede/glemte papirer med personoplysninger

Manglende overholdelse

Overtrædelse af denne politik kan få ansættelsesretlige konsekvenser i form af advarsel, opsigelse eller bortvisning afhængig af overtrædelsens karakter.

Opfølgning

Ad-Hoc Projekt måler, vurderer og følger op på informationssikkerhedsområdet på følgende måde:

- Løbende opfølgning på hændelser inden for IT-sikkerhed
- Opfølgning på vidensniveau inden for IT-sikkerhed i virksomheden i form af fx tests af medarbejdernes bevidsthed om IT-sikkerhed (awareness- eller phishing-tests)
- Løbende vurderinger af sikkerhedsaspekter i forbindelse med nye projekter, anskaffelser og ændringer
- Årlige/periodiske gennemgange af risikovurderingerne og -håndteringsplanen
- Gennemførelse af interne kontroller (auditeringer) og uafhængige tredjepartsevalueringer af informationssikkerheden i virksomheden

Senest opdateret marts 2024

Ad-Hoc Projekt ApS – Vestergade 9, 6520 Toftlund
Tlf: 7735 5000 – Mail: Kontakt@ad-hoc-projekt.dk – CVR-nummer: 4384 3230