TYPOCONSULT

IT Sikkerhedspolitik

TypoConsult A/S

2023-12-20, version 8

Versionslog

Versionsloggen angiver ændringerne i de forskellige versioner af aftalen.

Version	Ændringer	Dato	Ansvarlig
8.0	Der er foretaget følgende tilføjelser og ændringer i forhold til version 7: • 3. Fysisk sikkerhed og adgang til kontoret • 4. Fysisk sikkerhed og adgang til hosting centret • 18. Netværkskonfiguration på hosting miljøet • 29. Risikoanalyse og defencefile • 30. Funktionalitetstests med persondata	2023-12-20	Kristian Storm-Jørgensen
7.0	Der er foretaget følgende tilføjelser og ændringer i forhold til version 6: • 13. Administration af brugeradgange til systemer • 15. Styring af sikkerhedsbrud	2022-12-15	Kristian Storm-Jørgensen

1. Målsætning/formål

Sikkerhedspolitikken skal til enhver tid understøtte TypoConsults værdigrundlag og vision samt de strategiske mål. Hensigten med sikkerhedspolitikken er at tilkendegive over for alle, som har en relation til TypoConsult, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer.

TypoConsult ønsker derfor at opretholde og løbende udbygge et IT sikkerhedsniveau med høje krav, som skitseres i den til enhver tid gældende danske og europæiske databeskyttelsesret. Der er ligeledes indgået samarbejdsaftaler med kunderne, der forpligter til at opretholde et højt sikkerhedsniveau.

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at TypoConsult fremstår troværdig både nationalt og internationalt. For at fastholde TypoConsults troværdighed skal det sikres, at information behandles med fornøden fortrolighed, og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemer betragtes, næst efter medarbejderne, som TypoConsults mest kritiske ressource. Der lægges derfor vægt på driftsikkerhed, kvalitet og overholdelse af lovgivningskrav. Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at TypoConsults kunders data, medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Alle personer betragtes som værende en mulig årsag til brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

Målene er:

- at opnå høj driftsikkerhed med høje oppetidsprocenter og minimeret risiko for nedbrud og datatab.
- at opnå fortrolig behandling, transmission og opbevaring af data.
- at opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer.
- at opnå en gensidig sikkerhed omkring de involverede parter.
- at opnå en sikkerhed for gensidig og dokumenterbar kontakt.

Regler og retningslinjer for sikkerhedspolitikken skal løbende indarbejdes i de relevante gældende regler på personalepolitikkens område.

2. Gyldighedsområde

Politikken er gældende for alle TypoConsults informationsrelaterede aktiviteter, herunder udvikling, implementering, hosting og support, uanset om disse udføres af ansatte i TypoConsult eller af samarbejdspartnere. Dette inkluderer f.eks. alle data om personer, data om finansielle forhold, alle data som bidrager til administrationen af virksomheden, samt informationer som er overladt til TypoConsult af andre.

Sikkerhedspolitikken har gyldighed for alle ansatte i TypoConsult og al anvendelse af TypoConsults informationsaktiver.

3. Fysisk sikkerhed og adgang til kontoret

Medarbejdere får ved ansættelsen udleveret nøgler til gadedøren og til TypoConsults dør til kontoret. Derudover udleveres en personlig kode, som skal benyttes til at aktivere og deaktivere alarmen til kontoret. I kontorets åbningstid skal hoveddøren til TypoConsult være låst med øverste lås, så uvedkommende ikke bare kan gå ind. Udenfor kontorets åbningstid skal hoveddøren og døren til bagtrappen altid være låst med begge låse. Sidste medarbejder skal sikre, at alle vinduer er lukkede og at alle låse i hoved- og bagdør er låst, at kaffemaskinerne og lyset er slukket og at alarmen er aktiveret, når kontoret forlades.

Sættes alarmen i gang ved et uheld, skal de udleverede procedurer følges. Ved udlevering af alarm instruktionerne, oplyses en adgangskode, som skal oplyses til vagten ved opkald for annullering af alarmen.

Alarmsystemet og overvågningsservicen leveres af Verisure.

4. Fysisk sikkerhed og adgang til hosting centret

TypoConsults servere står fysisk hos Fuzion A/S, Niels Bohrs Vej 35, 8660 Skanderborg. Fysisk adgang til serverne kræver, at personerne er godkendte og clearet. Vores hosting partner fra WebHotel Danmark, Palle Nielsen, er godkendt til fysisk adgang til serverne.

Alle adgangstilladelserne gennemgås af den personaleansvarlige, når en ny medarbejder starter eller når en medarbejder stopper. Er der ingen fratrædelser eller ansættelser, så gennemgås tilladelserne årligt.

5. Adgang til Internet og WLAN

Internettet er som udgangspunkt at betragte som et arbejdsværktøj, der anvendes til opgaveløsning.

Privat brug af Internet i arbejdstiden skal begrænses til et minimum. Udenfor arbejdstiden er det tilladt at benytte virksomhedens Internet til private formål. Aktiviteter som kræver installation af software er ikke tilladt.

Der eksisterer altid en vis virusrisiko ved almindelig brug af Internettet. Virusrisikoen eksisterer specielt, når der downloades filer m.v. Medarbejdere skal derfor være yderst påpasselige ved download af filer - specielt fra ukendte afsendere.

Det er ikke tilladt at downloade eller distribuere software. Såfremt det viser sig, at download af software er nødvendig af arbejdsmæssige årsager, skal dette altid foregå ifølge aftale med ledelsen.

Trafik på Internettet bliver logget med henblik på netværksanalyse og datasikkerhed.

TypoConsult har to netværk 1) TC1 og 2) TC Guest. Kun TypoConsult medarbejdere må få adgang til TC1, og koden udleveres af ledelsen.

Ved udførelse af arbejde fra en hjemmearbejdsplads skal tilgang til udviklingsmiljøerne foregå via TypoConsults VPN adgang. Udstedelse af VPN adgang foretages af ledelsen.

6. Godkendelsesprocedure ved anskaffelser

Alle indkøb af software og abonnementer skal aftales og godkendes af TypoConsults ledelse. Softwarelicenser skal samles og købes på en TypoConsult konto, og derfra kan en udvalgt medarbejder tage rollen som administrator af licenserne, og uddelegere adgange til de enkelte medarbejdere.

7. Tavshedserklæringer

Medarbejdere må ikke besvare henvendelser fra en registreret bruger på en af vores kunders løsninger. Hvis det skulle ske, skal kunden underrettes. Henvendelser fra myndigheder vedr. en kundes løsning skal ligeledes meddeles kunden.

Medarbejdere må ikke dele personoplysninger med eksterne leverandører med mindre at leverandøren er en godkendt underleverandør for den pågældende kunde. Kundens kontaktperson skal per e-mail bekræfte, at en underleverandør er godkendt.

8. Databehandleraftaler

Ved samarbejder med nye kunder skal der indgås en databehandleraftale, som definerer under hvilke instrukser TypoConsult må arbejde med deres informationer og herunder specielt persondata. I tilfælde af tvivl om en kundes instruks, skal TypoConsults ledelse kontaktes, så opgaven kan tjekkes med den pågældende databehandleraftale.

9. Eksterne samarbejdspartnere

TypoConsults samarbejdspartnere er underlagt de samme tavshedserklæringer som TypoConsults medarbejdere. Samarbejdspartnere skal, så vidt det er muligt, ikke have adgang til vores kunders data og informationer. Såfremt opgaven kræver dette, skal kunden give sit samtykke hertil.

10. Medarbejdersikkerhed

Alle medarbejdere skal have læst seneste version af IT sikkerhedspolitikken, og have modtaget uddannelse, træning og oplysninger om krav til informationssikkerheden. Review og dokumentation på opdateringen foretages i forbindelse med TypoConsults årlige seminar eller efter behov.

11. Styring af driftsmiljøet

Driftsmiljøet drives i samarbejde med WebHotel Danmark (WebHot), og de fysiske servere er placeret hosFuzion A/S, Niels Bohrs Vej 35, 8660 Skanderborg. WebHot varetager drift, service, backup og overvågning af løsningerne. Retningslinjerne for driftsafviklingen er beskrevet i vores dokument for retningslinjer for driftsafvikling.

Ved problemer eller nedbrud tager WebHot kontakt til TypoConsults IT-chef (Claus Harup) eller den øvrige ledelse (Kristian Storm-Jørgensen). TypoConsult er altid den primære kontakt til vores kunder.

12. Sikkerhedskopiering og backup

WebHot står for backup og sikkerhedskopiering af udviklings- og driftsmiljøerne. De enkelte medarbejdere skal ikke selv sørge for en lokal backup af egen kode. Andre filer og dokumenter gemmes på TypoConsults Google Drive, og der kan også tages lokal backup på en NAS eller ekstern harddisk, såfremt den opbevares forsvarligt og aflåst på kontoret.

Dropbox og lignende services må ikke benyttes til backup formål.

13. Administration af brugeradgange til systemer

TypoConsults ledelse administrerer og tildeler adgange til systemer og licenser til software:

- Adobe
- Bitwarden
- ClickUp
- Docker
- e-conomic
- Figma
- GitHub
- Git
- Google (e-mail, kalender etc)
- Microsoft 365
- Notion
- Packagist
- PhpStorm
- Rollbar
- Slack
- VPN
- Workbook (Deltek)

Tildeling af adgange bør udelukkende ske ud fra et arbejdsbetinget behov.

14. Datamedier på den personlige arbejdsplads

Det er ikke tilladt at benytte datamedier til opbevaring af data med personlige oplysninger, med mindre datamedierne opbevares aflåst og utilgængeligt.

Scannes dokumenter med personlige data på TypoConsults scanner til en USB stick eller et hukommelseskort, så skal filerne slettes efterfølgende, så filerne ikke er tilgængelige for andre, der på et senere tidspunkt benytter mediet.

15. Styring af sikkerhedsbrud

Ved sikkerhedsbrud på en kundes løsning skal kunden underrettes jf. den pågældende databehandleraftale. Såfremt et sikkerhedsbrud identificeres, skal dokumentation ligeledes igangsættes for at afdække omfanget af sikkerhedsbruddet.

I tilfælde af sikkerhedsbrud følges procedurerne fra vores Risikoanalyse og defencefile, og brud skal dokumenteres med templaten til 'Underretning om incident'.

Ved databrud hos TypoConsult og vores egne data, skal ledelsen (Claus Harup / Kristian Storm-Jørgensen) underrettes. Kristian Storm-Jørgensen underretter Datatilsynet.

16. Elektronisk post, (e-mail)

Hver medarbejder har en e-mail adresse af formen xxx@typoconsult.dk. E-mail adressen er som udgangspunkt beregnet til arbejdsrelateret brug, men det er tilladt at sende og modtage private e-mails.

Der gøres opmærksom på både indgående og udgående post til/fra TypoConsults systemer, bliver logget og kopieret med henblik på data- og netværkssikkerhed. Opmærksomheden henledes i særdeleshed på at ledelsen i særlige situationer kan læse/tilgå indholdet af den enkeltes medarbejders postkasser.

17. Andre Internet-relaterede services

Det er ikke tilladt at køre privat software eller private services på virksomhedens netværk.

I tilfælde hvor brug af specielle programmer eller services skal benyttes f.eks. i forbindelse med kundekommunikation, vil der i hvert tilfælde skulle gives godkendelse til brug af denne pågældende service for den periode hvor projektet/opgaven strækker sig. Godkendelse gives af TypoConsults ledelse.

En særlig godkendelse til brug af en sådan service, er en specifik godkendelse til det enkelte projekt. Det medfører ikke, at disse services må bruges privat eller i forbindelse med andre kunder uden en godkendelse fra ledelsen.

18. Netværkskonfiguration på hosting miljøet

Af sikkerhedsmæssige grunde er der på FireWall niveau lukket for flest mulige indgående og udgående services. I følge aftale med ledelsen kan/vil der blive åbnet for de services, der er nødvendige for at udføre den/de opgaver den enkelte medarbejder skal løse.

Åbne services/porte i FireWallen er ikke ensbetydende med en godkendelse til brug af den pågældende service. Således betyder det ikke, at brug af tjenester der er mulige gennem FireWallen er tilladte tjenester. Retningslinjerne for hvilke tjenester der er godkendte, gælder uanset om at det er muligt at benytte andre tjenester.

Kontorets FireWall serviceres af KES-Net, så den løbende bliver sikkerhedsopdateret.

Netværkskonfiguration på vores hosting miljø varetages af WebHot, som er ansvarlig for sikkerheden. Sikkerhed og adgang til TypoConsults interne netværk varetages af TypoConsults tekniske chef, hvis ikke opgaven og ansvaret er uddelegeret til en fortrolig medarbejder.

19. Registrering / logging og overvågning

Som udgangspunkt kan det forventes at al aktivitet på virksomhedens interne net samt på virksomhedens gateways logges, med henblik på at analysere brug og evt. misbrug af netværket.

Virksomhedens ledelse er den eneste part, der har bemyndigelse til at igangsætte en sådan registrering. Det er således ikke tilladt for medarbejdere (uden godkendelse) at logge eller registrere aktivitet på netværket eller på anden måde at forsøge at tilgå informationer der ikke har oprindelse hos eller destination til medarbejderen selv.

20. Uautoriseret adgang

Ethvert forsøg på at tiltvinge sig uautoriseret adgang til dele af virksomhedens data er forbudt, med mindre det på forhånd er godkendt af ledelsen, at lave en sådan test af sikkerhedssystemet. Dette forbud gælder uanset hensigten med forsøget på adgangen.

21. Underretning

Såfremt der skulle opstå mistanke om eller ske sikkerhedsbrud i forbindelse med nogle af vores kunders løsninger, så skal kunderne underrettes jf. retningslinjerne i den pågældende kundes databehandleraftale.

22. Eksterne besøgende

I det omfang det er praktisk muligt, skal det i videst muligt omfang sikres, at eksterne personer, der tilkobler sig virksomhedens netværk skal være bekendt med hovedpunkterne i disse retningslinjer. Eksterne brugere må kun få adgang til TypoConsults gæstenetværk (TC1 Guest).

23. Filarkiver / Shares

Fælles og personlige filarkiver kan være beskyttet med adgangsbegrænsninger. Uanset om et givent filområde er adgangsbeskyttet eller ej, er det strengt forbudt at forsøge at tilgå dokumenter og information, som ikke er tiltænkt oplyst til den enkelte medarbejder.

Bevidste forsøg på uautoriseret adgang til filer vil blive betragtet som grov omgåelse af reglerne omkring intern sikkerhed, uanset om de pågældende dokumenter er beskyttet med adgangsbegrænsning eller ej.

24. Virus scanning og personlig firewall

Det er et krav, at hver medarbejder kører en fungerende virusscanning på sin egen computer, der løbende checker downloads fra internettet. Virusscanning på medarbejderes computer må kun deaktiveres i sjældne tilfælde, hvor en konkret situation kræver det.

Det burde ikke være nødvendigt at køre personlig firewall på maskinerne på det interne netværk, men det er tilladt i det omfang det ikke umuliggør brugen af de programmer der bruges internt.

25. Password procedure

TypoConsults medarbejdere må ikke dele deres personlige passwords med andre. Der er dog undtagelse i de tilfælde, hvor der oprettes brugerprofiler til testformål på vores kunders løsninger. Admin login i TYPO3 backenden må kun ske via login med Bitwarden.

BitWarden skal benyttes internt til at styre admin logins. BitWarden skal benyttes som password manager til TYPO3 backend admin-adgang samt til andre relevante credentials. Adgangskoder må ikke lagres i browsere.

26. Adgang til produktions- og udviklingsmiljøer

Det påhviler alle medarbejdere med shell adgang til nogle af TypoConsults egne eller kunders servere, at behandle denne adgang med yderste agtpågivenhed. Al shell adgang foregår via SSH protokollen.

Alle servere er opsat med firewall, således at man kun kan få SSH adgang fra bestemte IP-adresser. For ansatte hos TypoConsult er der adgang fra hovedkontorets IP-adresse, samt via en VPN løsning til brug uden for kontoret. Denne VPN-løsning er yderligere sikret med brugernavn og adgangskode.

VPN-adgangen til kontorets netværk og IP-adresse styres via vores MikroTik Firewall/Router. Opdatering af Soft- og firmware varetages via en aftale med KES Net. VPN credentials opbevares kun i vores generelle password manager (Bitwarden).

Hvis shell adgangen til serverne er blevet kompromitteret eller der opstår mistanke om uretmæssige forsøg på adgang, påhviler det medarbejderen straks (døgnet rundt) at informere ledelsen. Således at adgangen til de berørte servere kan spærres og de nødvendige tiltag foretages.

27. Offentliggørelse af kode og andet arbejde

Ingen har tilladelse til at offentliggøre eller videredistribuere materiale, der er udviklet eller produceret i regi af TypoConsult, uden at det på forhånd er godkendt af ledelsen. Således må ingen udviklede extensions, kodestumper eller noget andet materiale udleveres til andre end evt. den specifikke kunde, der har finansieret opgaven. Ingen extensions må publiceres på TER eller i øvrigt lægges offentligt tilgængeligt - uden dette er godkendt.

28. Adfærd og kommunikation i maillister/nyhedsgrupper

Medarbejdere har adgang til TYPO3 officielle maillister/news-servere. Når en medarbejder deltager i en diskussion/debat/tråd på en af disse newslister skal det indskærpes, at der ikke kan/må skelnes mellem hvad der er medarbejderens personlige holdning, og hvad der er TypoConsults holdning.

Man kan således IKKE skrive på disse maillister som privatperson – ej heller fra private e-mailadresser eller i anonymiseret form. Enhver ”optræden” i officielle TYPO3 kommunikationsfora skal ske med repræsentation af TypoConsults officielle holdninger til det pågældende spørgsmål, og såfremt medarbejderen på nogen måde er det mindste i tvivl om hvorvidt formulering er i overensstemmelse med TypoConsult holdning, bør indlægget godkendes af en person fra ledelsen INDEN afsendelsen.

Det skal noteres, at deltagelse i enhver ”tråd” med et negativt ladet indhold, uanset om det er negativt omkring TYPO3, TypoConsult, andre leverandører eller helt andre ting – kun kan ske med ledelsens accept.

29. Risikoanalyse og defencefile

Risikoanalysen er et dokument som opdateres løbende over året, da der kan opstå nye risici og trusler, som vi skal forholde os til. Den skal give et overblik over de mulige trusler, som TypoConsult skal forholde sig til og iværksætte nødvendige foranstaltninger.

På vores årlige medarbejderseminar eller efter behov, vil analysefilen bliver gennemgået, diskuteret og opdateret. Alle medarbejdere er forpligtet til at bidrage til risikovurdering over året og på seminaret, så vi opsamler aktuel viden om risici og trusler i forhold til det aktuelle risikobillede.

30. Funktionalitetstests med persondata

Ved lokal udvikling af funktioner til håndtering af persondata er nødvendigt at teste funktionaliteten med. Af sikkerhedsmæssige hensyn kræves det, at der benyttes kunstige data eller en anonymiseret udgave af data fra produktionsmiljøet.

31. Kontrol

Medarbejderne bekræfter ved underskrift på et versionslog dokument at:

- have læst og forstået retningslinjerne for brugen af de interne IT systemer i seneste gældende version af TypoConsults IT sikkerhedspolitik.
- har fået mulighed for at stille uddybende spørgsmål til punkter i regelsættet.
- være bekendt med at grov overtrædelse/misligholdelse af regler og/eller producerer i dette sæt regler kan påvirke ansættelsesforholdet og i yderste konsekvens medføre bortvisning og politianmeldelse.