

IT-politik for [Virksomhedens navn]

En GDPR-klar starter-skabelon til danske SMV'er. Udfyld felterne, tilpas afsnittene til jeres virkelighed og få vedtaget politikken af ledelsen. Skabelonen dækker brug af IT-udstyr, adgangskoder, e-mail og internet, hjemmearbejde, behandling af persondata, hændelseshåndtering og sanktioner.

Sådan bruger I skabelonen

- Erstat alle felter i [klammer] med jeres egne oplysninger.
- Slet eller tilføj afsnit, så politikken matcher jeres faktiske drift.
- Få politikken godkendt af direktionen og dateret før udrulning.
- Gennemgå politikken med alle medarbejdere og indhent kvittering for læsning.
- Revider mindst én gang om året — eller når jeres IT-setup ændres væsentligt.

Vigtigt: Denne skabelon er udarbejdet som et praktisk udgangspunkt og erstatter ikke juridisk rådgivning. Tilpas formuleringerne til jeres branche, størrelse og behandlingsaktiviteter — særligt hvis I er omfattet af NIS2 eller behandler følsomme persondata.

1. Formål og omfang

Formålet med denne IT-politik er at sikre, at [Virksomhedens navn] benytter IT på en sikker, lovlig og effektiv måde. Politikken gælder for alle medarbejdere, vikarer, praktikanter, konsulenter og andre, der har adgang til virksomhedens IT-systemer og data.

Virksomhedens navn: [CVR-nr.]

Politik-ejer: [Titel og navn, fx adm. direktør]

Dato for ikrafttræden: _____

Næste revisionsdato: _____

2. Brug af IT-udstyr

Virksomhedens IT-udstyr (computere, telefoner, tablets, eksterne diske mv.) stilles til rådighed for arbejdsrelaterede formål. Begrænset privat brug er tilladt, så længe det ikke påvirker arbejdet eller udsætter virksomheden for risiko.

Medarbejderen skal:

- Behandle udstyret med omhu og opbevare det forsvarligt — ikke synligt i bil eller offentlige steder.
- Låse skærmen, når arbejdspladsen forlades (Win+L eller Ctrl+Cmd+Q).
- Kun installere software, der er godkendt af IT-afdelingen eller [IT-leverandør].
- Straks melde tab, tyveri eller mistanke om kompromittering til [kontaktperson].
- Aflevere alt udstyr og fjerne adgange ved fratrædelse.

3. Adgangskoder og MFA

- Adgangskoder skal være mindst 14 tegn og må ikke genbruges på tværs af tjenester.
- Brug en password-manager til at gemme og generere unikke kodeord (fx 1Password, Bitwarden).
- Multi-faktor-autentificering (MFA) er obligatorisk på alle tjenester der understøtter det — som minimum Microsoft 365, e-mail, økonomisystem og remote-adgang.
- Del aldrig kodeord, heller ikke med kolleger eller IT-support. Brug i stedet officielle delings-mekanismer.
- Skift kodeord straks ved mistanke om kompromittering — ikke efter en fast tidsplan.

Godkendt password-manager: _____

Ansvarlig for brugeradministration: _____

4. E-mail og internet

- Vær opmærksom på phishing — vurder altid afsender, links og vedhæftninger, særligt ved hastværk eller pengetransaktioner.
- Videre-send aldrig forretningskorrespondance til private e-mailkonti.
- Følsomme oplysninger (CPR, kontooplysninger, sundhedsdata) sendes krypteret eller via sikker tjeneste — ikke i almindelig e-mail.
- Privat brug af internettet er tilladt i begrænset omfang og må ikke omfatte ulovligt, krænkende eller forretningsskadeligt indhold.
- Mistænkelige e-mails rapporteres til [phishing-kontakt] — slet ikke uden at melde.

Phishing-kontakt (e-mail): _____

5. Hjemmearbejde og rejser

- Anvend kun virksomhedens udstyr til arbejdsopgaver — undgå at gemme firmadata på private enheder.
- Brug VPN ved adgang til interne systemer fra offentlige netværk (cafeer, hoteller, tog).
- Hold familie og besøgende ude af videomøder med fortrolige oplysninger.
- Lås skærm, opbevar udstyr forsvarligt og medtag ikke unødvendige fortrolige dokumenter på rejser.
- Print kun fortrolige dokumenter, hvis det er nødvendigt — og makulér dem efter brug.

Godkendt VPN-løsning: _____

6. Behandling af persondata (GDPR)

Vi behandler kun persondata til legitime, dokumenterede formål og opbevarer dem ikke længere end nødvendigt. Alle medarbejdere skal kende deres ansvar for at beskytte persondata, de håndterer i det daglige.

- Persondata må kun tilgås, hvis det er nødvendigt for opgaven.
- Persondata må kun deles med tredjeparter, hvis der findes en databehandleraftale (DPA).
- Følsomme persondata (helbred, fagforening, biometri mv.) kræver særlig hjemmel og sikres med kryptering og begrænset adgang.
- Brug aldrig private cloud-tjenester (Dropbox, Gmail, WeTransfer) til firmadata uden godkendelse.
- Sletning af persondata følger virksomhedens slettefrister — se afsnit 7.

Dataansvarlig: _____

DPO eller GDPR-kontakt (hvis udpeget): [Ikke obligatorisk for SMV]

7. Opbevaring, backup og sletning

- Firmadata gemmes i godkendte systemer — fx OneDrive, SharePoint eller [ERP-system] — ikke lokalt på enheder.
- Backup tages dagligt og opbevares mindst [30] dage. Backup testes minimum [hver kvartal].
- Persondata slettes eller anonymiseres efter [angiv frist, fx 3 år efter kundeophør] — medmindre lovkrav siger andet.
- Ved fratrædelse arkiveres medarbejderens mailboks i [angiv periode, fx 90 dage] og slettes derefter.

Godkendt fil-lager: _____

Backup-frekvens og opbevaringsperiode: _____

Slettepolitik for kundedata: _____

8. Hændelseshåndtering og databrud

Et databrud kan være tab af udstyr, uautoriseret adgang, ransomware, fejl-afsendelse eller mistanke om phishing. Alle hændelser meldes straks til [kontaktperson] — også ved den mindste tvivl.

De første 24 timer:

- Meld hændelsen til intern kontakt OG [IT-leverandør].
- Isolér berørt udstyr — sluk ikke, men afbryd netværk hvis muligt.
- Dokumentér hvad der er sket, hvornår, og hvilke data der kan være berørt.
- Dataansvarlig vurderer, om hændelsen skal anmeldes til Datatilsynet inden 72 timer.
- Berørte personer underrettes, hvis hændelsen indebærer høj risiko.

Intern hændelses-kontakt: _____

IT-leverandør / hotline (24/7): _____

9. Awareness og oplæring

- Alle nye medarbejdere gennemgår en kort IT-sikkerheds-introduktion ved onboarding.
- Mindst én gang om året afholdes phishing-test og awareness-træning.
- Politikken læses og bekræftes af alle medarbejdere — kvittering arkiveres af [HR-ansvarlig].

10. Sanktioner ved overtrædelse

Overtrædelse af denne IT-politik kan medføre advarsel, opsigelse eller bortvisning afhængigt af karakter og omfang. Forsætlige eller groft uagtsomme handlinger kan derudover medføre politianmeldelse og krav om erstatning. Sanktioner følger virksomhedens øvrige personalepolitik.

Godkendelse

IT-politikken er godkendt af [Virksomhedens navn] med virkning fra ovennævnte dato.

Dato: _____

Navn og titel: _____

Underskrift: _____

Skabelon udarbejdet af IT-Hjælpen — din eksterne IT-afdeling for SMV'er. Brug for hjælp til at få politikken til at leve i hverdagen? Book en gratis IT-gennemgang på it-hjaelpen.com/kontakt.