Skabelon for IT-sikkerhedshåndbog

Følgende dokument er en skabelon til udarbejdelse af en IT-sikkerhedshåndbog.
IT-sikkerhedshåndbogen er en medarbejdernær vejledning som udmønter organisationens IT-sikkerhedspolitik i konkrete retningslinjer for medarbejderen. Dokumentet er én af flere skabelon-dokumenter, som indgår i det IT-sikkerhedsmateriale, som alle organisationer bør have ift. overholdelse af NIS2.

Vi har i Lakeside lavet en række skabeloner, som du er velkommen til at bruge. Skabelonerne er tiltænkt SMV’er med produktion, men kan sagtens bruges af organisationer uden produktion (OT). Skabelonerne er udarbejdet med udgangspunkt i små og mellemstore forsyningsselskaber.

* IT-sikkerhedspolitik
* Nærværende IT-sikkerhedshåndbog
* IT/OT-leverandør sikkerhedspolitik
* IT/OT-leverandør tjekliste
* Risikostyringspolitik og Risikolog
* Hændelseshåndteringsprocedure og Hændelseslog
* Kriseberedskabspolitik, -planer og -skabeloner

Skabelonerne for de øvrige dokumenterne kan findes og downloades på [www.lakeside.dk/publikationer](http://www.lakeside.dk/publikationer)

**Sådan bruger du skabelonen**

* Tekster med gråt og i firkantede klammer er vejledningstekster, som slettes ved endt redigering.
* <organisation> er en dokument-egenskab. Den kan rettes under Filer / Egenskaber / Brugerdefineret (nederste tekstboks) og derefter opdatere alle felter i hele dokumentet (vælg alt og højreklik).
* Alle tekster kan ændres efter behov og som tilpasning til din organisation. Alle tekster med gult bør du ændre eller som minimum forholde dig til.
* Kontaktinformation og organisation skal opdateres i sidehoved og sidefod. OBS! Organisation og logo på forsiden er også i en sidefod.

Dato | Version X.X

IT-sikkerheds håndbogen

Revisions- og Godkendelseshistorik

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer | Godkendt |
| [0.0] | [dd.mm.yy] | [INT] |  | [dato / navn] |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Kontaktpersoner

|  |  |
| --- | --- |
| Fornavn Efternavn (initialer)Skriv din titel her, fx konsulentTlf.: +45 xxxx xxxxxxx@domæne.dk<Organisation> | Fornavn Efternavn (initialer)Skriv din titel her, fx konsulentTlf.: +45 xxxx xxxxxxx@domæne.dk<Organisation> |

Indholdsfortegnelse

[1 Indledning 3](#_Toc185567065)

[2 Medarbejderansvar 3](#_Toc185567066)

[3 Fortrolighed 3](#_Toc185567067)

[4 Brug af mail 4](#_Toc185567068)

[4.1 Autoriserede brugere 4](#_Toc185567069)

[4.2 Upassende indhold i e-mails 5](#_Toc185567070)

[4.3 Adskillelse af privatliv og arbejde 5](#_Toc185567071)

[4.4 E-mail sikkerhed 5](#_Toc185567072)

[4.5 Brug af sikker mail 6](#_Toc185567073)

[4.6 Arkivering af dokumentation 6](#_Toc185567074)

[4.7 Opmærksomhed ved modtagelse af mail 7](#_Toc185567075)

[5 Brug af internettet 7](#_Toc185567076)

[6 Brug af enheder 8](#_Toc185567077)

[6.1 Software (programmer og app’s) 8](#_Toc185567078)

[6.2 Brug af telefon 8](#_Toc185567079)

[6.3 Opmærksomhed ved brug af enheder 9](#_Toc185567080)

[6.4 Passwordpolitik 9](#_Toc185567081)

[6.5 Password til pc 9](#_Toc185567082)

[6.6 Password – specifikt system 10](#_Toc185567083)

[6.7 Passwordmanager 10](#_Toc185567084)

[7 Print 11](#_Toc185567085)

[8 Overvågning og logning 11](#_Toc185567086)

[9 Rapportering af hændelser 11](#_Toc185567087)

[9.1 Det kan der ske 12](#_Toc185567088)

# Indledning

Denne IT-sikkerhedshåndbog indeholder en række regler, retningslinjer og vejledninger til hvordan medarbejdere overholder s IT-sikkerhedspolitik.

# Medarbejderansvar

Det er den enkelte medarbejders ansvar at efterleve sikkerheden omkring IT-anvendelsen i jævnfør IT-sikkerhedspolitikken og nærværende IT-sikkerhedshåndbog.

Alle medarbejdere er desuden forpligtiget til at gøre sig bekendt med de til enhver tid gældende privatlivspolitikker. Eksterne privatlivspolitikker (kunder, jobansøgere, cookie-politik) er publiceret på hjemmesiden link. Den interne privatlivspolitik (medarbejdere) udleveres sammen med ansættelseskontrakt og forefindes endvidere på fællesdrev / intranet.

Alle medarbejdere er ansvarlige for at rapportere om eventuelle sikkerhedsbrud eller mistanke herom til nærmeste leder og IT-sikkerhedsfunktionen.

Bevidst brud på de nævnte politikker og retningslinjer, anses som en væsentlig overtrædelse af kontraktforholdet mellem og medarbejderen, og vil medføre disciplinære foranstaltninger, herunder også afslutning af ansættelsesforholdet.

# Fortrolighed

Medarbejdere underskriver en fortrolighedserklæring med. Fortrolighedserklæringen er gældende både under og efter ansættelse.

Medarbejdere ved skal i arbejdstiden være opmærksomme på, at udefra kommende (leverandører, kunder, servicemedarbejdere o.l.) ikke lytter eller ser med, når der arbejdes med kundedata og/eller når kundernes data drøftes mellem medarbejderne.

Papirer med kunde- eller medarbejderoplysninger må ikke ligge frit fremme på skrivebordet, når medarbejderen forlader skrivebordet og udskrifter skal hentes i printeren straks disse er udskrevet.

I fritiden skal medarbejdere ved være opmærksomme på den tavshedspligt man er pålagt, hvor kunde og/eller medarbejderdata ikke må deles, drøftes eller uforvarende komme til 3. mands (familie, venner, samt tilfældigt forbipasserende) kendskab.

# Brug af mail

Der stilles en personlig e-mailadresse til rådighed for alle medarbejdere, bestyrelsesmedlemmer og leverandører, hvor det måtte være relevant og brugbart for udførelsen af deres arbejdsopgaver.

Ligesom alt anden teknologi kan brugen af e-mail skabe en sikkerhedsrisiko, hvis den bliver brugt på en upassende, eller på anden måde ikke korrekt, vis.

Formålet med nedenstående retningslinjer er at beskrive de regler der er gældende for brugen af e-mail i og derved mindske disse risici mest muligt.

Brugerne skal være opmærksomme på at deres personlige virksomheds e-mailadresse og dertil hørende postkasse er s ejendom og at indholdet kan overvåges som beskrevet i afsnit *10 Overvågning og logning.*

## Autoriserede brugere

Det er alene brugere, der har fået godkendelse til at benytte en personlig virksomheds e-mailadresse, der må gøre brug af s e-mailsystem.

Autorisation gives ved henvendelse til ansvarlig for mail-systemet.

Uautoriseret brug af selskabets e-mailsystem er ikke tilladt.

Dette gælder for såvel det at gøre brug af en anden brugers e-mail eller at give adgang til andre uautoriserede personer.

Det gælder alene for fælles postkasser at flere brugere er autoriserede til at tilgå disse, se IT-sikkerhedspolitikken Bilag C.

## Upassende indhold i e-mails

Selskabets e-mail system må ikke bruges til at sende eller opbevare upassende indhold eller materiale.

Al visning eller distribution af upassende indhold via e-mail er ikke acceptabelt og vil medføre sanktioner.

|  |
| --- |
| Upassende indhold inkluderer:Pornografi/nøgenbilleder, religiøse eller racerelaterede nedsættende bemærkninger, kønsspecifikke nedsættende kommentarer, opmuntrende information om terror eller andre kriminelle handlinger, materiale omhandlende sekter, spil (gambling) eller ulovlige og/eller euforiserende stoffer.Definitionen af upassende indhold eller materiale dækker også over tekst, billeder eller andet medie, der med rimelighed kan siges at støde nogen på baggrund af race, alder, køn, religiøse eller politiske overbevisninger, oprindelsesland / etnisk oprindelse, handicap, seksuel præference eller andre kendetegn beskyttet ved lov. |

Enhver bruger der modtager en e-mail, de betragter som upassende har pligt til at melde dette til deres nærmeste leder eller IT-sikkerhedsfunktionen.

## Adskillelse af privatliv og arbejde

Medarbejdere skal som udgangspunkt ikke benytte deres arbejds-e-mail til privat brug.

 tillader, i begrænset omfang, at medarbejderne benytter selskabets e-mailadresse til private formål, hvilket er begrænset til modtagelse af private beskeder. Brugeren gøres igen opmærksom på at indholdet kan overvåges som beskrevet i afsnit *10 Overvågning og logning.*

 tillader brugerne til, i begrænset omfang, at tjekke deres private e-mail konti på enheder ejet af selskabet.

## E-mail sikkerhed

Uhensigtsmæssig brug af e-mail kan forårsage alvorlige sikkerhedsproblemer for en virksomhed.

Det forventes at alle brugere af s e-mail system tilgår systemet med årvågenhed under hensyntagen til følgende:

* Lad være med at åbne vedhæftede elementer fra ukendte afsendere, da de kan indeholde virus, Trojanske heste, spyware eller andet malware
* Lad være med at deaktivere installeret scannings- eller anden sikkerheds-software. Disse værktøjer er afgørende for beskyttelse af selskabets data
* Lad være med at sende fortrolige eller personfølsomme data via almindelig e-mail. Data skal anonymiseres eller Sikker e-mail benyttes.
* Tag stilling til indholdet i det du sender og om informationen skal afsendes i et ikke-redigerbart format (PDF det du ikke ønsker ændret på ved modtager).

Ved tvivl rådspørges den IT-ansvarlige.

Generelt bør det understreges at e-mail er at betragte som en åben kommunikationsplatform, da de fleste e-mails er sendt som ren tekst og derved nemt kan blive opsnappet. Almindelig e-mail er således ikke egnet til at blive brugt til fortrolige meddelelser og information, herunder også persondata relateret information.

## Brug af sikker mail

Sikker e-mail benyttes til udveksling af følsomme personoplysninger og fortrolige oplysninger.

Sikker e-mail er en krypteret mail man sender fra Outlook via selskabets sikre postkasser.

En Sikker e-mail bliver både krypteret (kodet, så det ikke kan læses af uvedkommende undervejs) og forsynet med en digital signatur (signeret så modtager er sikker på at mailen kommer fra ).

OBS 1: Modtagelse af Sikker-mail kræver at modtageren selv har en sikker postkasse.

OBS 2: Du skal være opmærksom på, at emnefeltet ikke krypteres i en sikker e-mail. Du må derfor ikke skrive følsomme eller fortrolige oplysninger som fx cpr-nummer i emnefeltet.

## Arkivering af dokumentation

Det forventes alle brugere holder indholdet af deres postkasse til et minimum.

**Alt materiale der skal fungere som dokumentation**, skal ikke opbevares i e-mail systemet men videreekspederes til fagsystem eller på server-drev.

**Alt materiale der indeholder personoplysninger**, skal ikke opbevares i e-mail systemet men videreekspederes til fagsystem eller på server-drev, eller slettes ved endt behandling.

Jf. Persondataforordningen (GDPR) skal selskabet være i stand til at udlevere alt registreret data på en person, hvorfor det er nødvendigt at dette kan fremsøges nemt via fagsystemerne.

## Opmærksomhed ved modtagelse af mail

Mange cyber-angreb foretages via tilsendte mails, og uopmærksomme modtagere af mails, så vi opfordrer til, at du er opmærksom, når du gennemgår din indbakke:

1. Åbn ikke mails du normalt aldrig får tilsendt med emner som f.eks.:
* du har vundet…
* du er udvalgt til…
* SKAT har brug for at du validerer dine kontaktoplysninger (el. andre myndigheder, hvor du ikke har oplyst din arbejdsmail)
* Tydeligvis er oversat af en maskine (som fx Google translate)
* Bekræft leveringsoplysninger på levering af din IPhone
1. Kommer mailen fra en tilsyneladende pålidelig kilde, skal det overvejes om der er en grund til at de skriver til dig
2. Tryk ikke på links i mails eller på hjemmesider du ikke ved hvad drejer sig om
3. Åbn ikke vedhæftede filer i mails du ikke ved hvad drejer sig om
4. Tjek afsender mailadressen ved at køre musen hen over afsender navn (sådan kan du tjekke om afsender også er den der skrives at det er).

# Brug af internettet

s medarbejdere har adgang til internettet. Internettet kan benyttes i det omfang, det er relevant for udførslen af arbejdsopgaven.

Upassende indhold, samt de øvrige forbud beskrevet i afsnit 4.3, gælder også for hjemmesider, hvorfor du bedes undlade at besøge sådanne hjemmesider.

I arbejdstiden må sociale medier kun anvendes til arbejdsmæssige relationer.

Som ansat hos forventes det, at du optræder loyalt over for selskabet, ledelsen og dine kolleger; også i din ageren på sociale medier.

Brugerne skal være opmærksomme på, at al internettrafik kan overvåges jf. afsnit 10 Overvågning og logning.

# Brug af enheder

Følgende afsnit gælder for arbejdsgiver betalte enheder, såsom pc’er, smartphones, tablets o. lign.

## Software (programmer og app’s)

Det er ikke tilladt brugerne selv at installere ikke-godkendte eller private programmer lokalt på pc eller andre enheder (mobiltelefon/IPad) eller på den administrative server.

Der stilles postkasse (e-mail), nødvendige fag- og tekst- / databehandlingssystemer, personligt drev samt adgangsstyrede fællesdrev til rådighed for løsning af arbejdsopgaven.

Opstår behov for yderligere programmer skal dette godkendes ved nærmeste leder for mest hensigtsmæssige installation samt licens indhentning.

Virksomhedsrelaterede data og dokumenter må ikke opbevares på ubeskyttede, usikre elektroniske lokationer, som fx Dropbox. Kontakt den IT-ansvarlige for at høre hvilke muligheder, der findes indenfor det sikrede miljø.

## Brug af telefon

Der er forbud mod egentlig privat anvendelse af telefonen, til betaling af private udgifter, herunder til donationer, deltagelse i sms-konkurrencer og lignende.

Medarbejderne skal være opmærksomme på, at kan indhente oplysninger om opkald og betaling af udgifter via telefonen med henblik på kontrol af, at ovenstående overholdes.

## Opmærksomhed ved brug af enheder

1. Lås altid din skærm når du går fra din pc, tablet, telefon og giv aldrig andre uovervåget adgang til enheden (lån fx ikke nogen din enhed for selv at udfylde kontaktinfo, tjekke forbrug etc.)
2. Sæt ikke en ukendt lagringsenhed (fx USB-nøgle) i din pc (finder du fx en USB-nøgle på p-pladsen skal du ikke forsøge at tjekke indholdet – aflever den til IT-sikkerhedsfunktionen)
3. Spørg hellere IT-sikkerhedsfunktionen en gang for meget end en gang for lidt hvis du bare er det mindste i tvivl
4. Spørg hellere IT-sikkerhedsfunktionen en gang for meget end en gang for lidt - det kan ikke siges for tit
5. Bærbare medier må ikke efterlades i bilen, men skal altid medbringes, så disse ikke risikere at blive stjålet ved indbrud i bilen, selv i dagtimerne.

## Passwordpolitik

Der er følgende krav til dit kodeord (password):

* Det skal være mindst 8 karakterer langt (men må gerne være længere)
* Det må ikke indeholde dele af dit navn, brugernavn, fødselsdato eller telefonnummer
* Det skal indeholde mindst 3 ud af flg. 4 kategorier:
	+ Store bogstaver (A-Z)
	+ Små bogstaver (a-z)
	+ Tal (0-9)
	+ Specialtegn. (,.!@?+-)
* Det skal være noget, du kan huske (brug fx en passwordsætning)

## Password til pc

Password skal skiftes hver 3. måned. Den enkelte medarbejder er ansvarlig for at anvende og udskifte koden, som anvendes ved login på arbejdsstationen/computeren.

### Vejledning til skift af password på PC

|  |  |
| --- | --- |
| 1. Tryk CTRL + ALT + DEL på dit tastatur
2. Vælg ”Skift en adgangskode”
3. Skriv din nuværende adgangskode (i feltet står ”Tidligere adgangskode”)
4. Skriv din nye adgangskode i feltet ”Ny adgangskode” og bekræft den i feltet ”Bekræft adgangskode”.
5. Tryk på enter
6. Adgangskoden er nu skiftet, og du skal fremover bruge den nye kode til at logge på med.
 | cid:image003.jpg@01D3677C.D6E16E20 |

## Password – specifikt system

[Vejledning: hvis I har andre systemer, hvortil der er behov for en specifik retningslinje for passwords. Ellers slettes afsnittet.]

## Passwordmanager

 stiller en passwordmanager til rådighed for alle medarbejdere, og medarbejderne opfordres til at benytte denne.

Brug af passwordmanager har flere fordele:

* Man skal kun huske ét password, men kan undgå at genbruge passwords på tværs af services, hvilket begrænser konsekvensen af et læk
* Passwordmanagers kan hjælpe en med at generere et stærkt password (men de er typisk ikke nemme at huske)
* Passwordmanagers kan advare brugere om, hvis deres passwords er lækket, så brugeren kan skifte det pågældende password.

Medarbejdere må ikke benytte browserens ’husk password’ funktion, medmindre den pågældende browser sættes op med kryptering og hovedpassword.

# Print

Ved udskrivning har vi mulighed for at benytte personlig brugerbakke (lageret udskrift med kode) og således minimere risikoen for at print med persondata kommer uvedkommende til kendskab.

Har du ikke brugerbakke, men ønsker det, kan du kontakte IT-sikkerhedsfunktionen, der vil sørge for oprettelse.

Gå aldrig fra dit skrivebord, hvis der ligger papirdokumenter o.l. med kundeoplysninger på bordet, men sørg altid for at sådanne papirdokumenter er låst inde, når du forlader dit skrivebord

# Overvågning og logning

Selskabets e-mailsystem og software stilles til rådighed for brugerne til brug for legitim arbejdsmæssig brug.

Det er ikke s politik at overvåge deres medarbejdere, men selskabet forbeholder sig af sikkerhedsmæssige årsager ret til at logge alle brugeres brug af e-mail og internet.

Loggen kan registrere internet- og mail trafik, af- og på-logning samt identificere associerede filer.

Selskabet kontrollerer ikke løbende brugernes IT-anvendelse, men kan i tilfælde af fx begrundet mistanke om misbrug, sikkerhedsbrud eller andre ulovligheder, væsentlige arbejdsmæssige årsager, driftsmæssige forhold / fejl eller i forbindelse med brugerens ophør, finde det nødvendigt at gennemføre en sådan kontrol.

# Rapportering af hændelser

Hvis der konstateres trusler mod s IT-ressourcer eller IT-bårne data eller der konstateres overtrædelser af elementer i IT-sikkerhedsmaterialet, skal dette hurtigst muligt meddeles den øverste IT-sikkerhedsansvarlige (direktøren), IT-sikkerhedsfunktionen eller nærmeste leder.

## Det kan der ske

s eksistensgrundlag og dermed virksomhedens arbejdspladser kan være truet af:

* data kan blive låst med krav om løsesum
* data kan blive solgt til kriminelle der ønsker at ramme Danmark med et angreb mod tjenester af væsentlig samfundsmæssig karakter (fx el, vand, varme, banker)
* branchens troværdig kan lide et knæk, hvis fjernvarmeværker havner på forsiden af dagbladene (og koste dyrt på fjernvarmeprisen)
* kan blive idømt bødestraf på op til 4% af selskabets omsætning (ca. 2,5 mio. kr.)
* hackere kan overtage kontrollen med produktionen

Ved grov uagtsomhed, ift. IT-sikkerhedspolitikken og medhørende retningslinjer, kan medarbejderen i yderste konsekvens risikere afskedigelse og politianmeldelse.