



TJEKLISTE

20 TEKNISKE MINIMUMSKRAV

# Få styr på jeres IT-sikkerhed

Kan du sætte flueben ved 20 tekniske  
minimumskrav?



**CapaSystems**  
...because time matters

## TJEKLISTE

Center for Cybersikkerhed, Digitaliseringsstyrelsen og Datatilsynet har kigget nøje på, hvilke basale dele af IT-sikkerheden, der bør fokuseres på nu og her.

**ALLE** virksomheder burde kunne sætte flueben ved 20 tekniske minimumskrav til IT-sikkerheden.

Målet er klart: Et fælles højt sikkerhedsniveau skal sikres.

Tjek her, hvor mange af kravene I kan sætte flueben ved:

### Klienter/PC'er (pkt. 1-7):

- Der skal implementeres firewall på alle klienter
- Klienter skal benytte "Always On VPN" fra eksterne netværk
- Klienters harddiske skal krypteres
- Der skal implementeres endpoint-beskyttelse på alle klienter
- Klienters OS og applikationer på klienten skal holdes sikkerhedsopdateret
- Alm. brugerkonti må ikke tildeles administrative rettigheder til klienten
- Klienter skal anvende det nyeste operativsystem



# TJEKLISTE

## Mail (pkt. 8-9):

- Der må kun anvendes godkendte mailrelays med autentifikation
- Kommunikation med mail-protokoller skal krypteres og anvende min. TLS 1.2
- Kommunikér problemet med børns adgang til maskinerne

## Autentifikation (pkt. 10):

- Myndighedens systemer over internettet skal anvende flerfaktor-autentificering

## Mobile enheder (pkt. 11-13):

- Anvend numerisk adgangskode på min. 6 cifre eller biometrisk identifikation
- MDM skal implementeres på alle mobile enheder
- Operativsystem og apps på mobile enheder skal holdes sikkerhedsopdateret

## Logning (pkt. 14):

- Krav om logning, log på systemer og tjenester på netværksservere



# TJEKLISTE

## Domæner (pkt. 15-17):

- DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden
- Myndigheden skal anvende en sikker DNS-tjeneste eller implementere anden løsning til beskyttelse mod adgang til kendte skadelige domæner
- DMARK REJECT policy implementeres på alle domæner tilhørende myndigheden

## Netværk (pkt. 18-20):

- Det interne WiFi-netværk skal være krypteret med min. WPA2
- Software på myndighedens internetvendte tjenester skal holdes sikkerhedsopdateret
- Adgang til jeres internetvendte tjenester, herunder hjemmesider, skal ske over en krypteret forbindelse

---

### Fik du sat alle 20 ✓?

Så er alt godt, og du har styr på IT-sikkerheden i jeres organisation. I opfylder ALLE de tekniske minimumskrav, der bør være på plads hurtigst muligt.

### Fik du sat færre end 20 ✓ ?

Du har brug for at se nærmere på tingene for at sikre det sidste omkring IT-sikkerheden i jeres organisation.



# Skal vi hjælpe med at sætte flueben?

## Kontakt os i dag.

+45 70 10 70 55

[info@capasystems.com](mailto:info@capasystems.com)

---

### Lad os hjælpe jer 8 skridt tættere på målet:

- **Firewall:** Implementering af firewall på alle klienter
- **Kryptering:** Kryptering af klienters harddiske
- **Opdatering:** Opdatering af klienters OS og applikationer
- **PAM:** Automatisk op- og nedskalering af brugerrettigheder
- **Nyeste OS:** Udrulning af de nyeste operativsystem
- **MDM:** Administration af mobile enheder - uanset platform
- **Luk huller:** Opdatering af operativsystem og apps på mobile enheder
- **Server:** Opdatering af software på internetvendte tjenester

*CapaSystems' løsninger har i over 25 år sikret og optimeret IT hos både danske og udenlandske virksomheder. Der er derfor rig mulighed for at trække på vores dybe indsigt og branchekendskab, da vi som dansk virksomhed har stærke kompetencer og ganske enkelt ved, hvad vi taler om.*