Anbefalinger om tekniske minimumskrav i kommuner 2024

De tekniske minimumsstandarder for kommuner er udarbejdet første gang under Sikkerhedsprogrammets partnerskab og vedligeholdes i samarbejde med et antal kommuner. Anbefalingerne har tidligere været inspireret af, og taget udgangspunkt i, listen over tekniske minimumskrav til statslige myndigheder fra 2020 og er efterfølgende blevet revideret i takt med opdatering af de statslige tekniske minimumskrav.

Om anbefalingerne

De statslige tekniske minimumskrav blev sidst opdateret i juli 2024. I den forbindelse er anbefalingerne om tekniske minimumsstandarder for kommuner blevet opdateret, så de nu følger de statslige med et par mindre kommunale justeringer. Der er fortsat en række anbefalinger, der kun gælder kommunerne, men de er blevet færre, da nogle af dem er overgået til statslige krav.

Baggrunden for at anbefale de statslige krav og ikke kun lade sig inspirere af dem er, at der er en forventning om, at der vil kunne komme krav om efterlevelse af disse ifm. implementeringen af NIS2 eller andre kommende lovgivninger på cybersikkerhedsområdet.

	Anbefaling	**Anvisninger**
Nr.	Klienter/Pcer: Anbefalingerne angår alle de stationære, bærbare og virtuelle computere, som har adgang til kommunens systemer.	
S1	Der skal implementeres firewall på alle klienter.	Anbefalingen er opfyldt, hvis 1) der er implementeret firewall på alle klienter hos kommunen og 2) kommunen aktivt har forholdt sig til nødvendig indgående og udgående trafik på klienten og 3) firewallpolitikken/konfigureringen kun tillader det, der er identificeret som nødvendigt jf. punkt 2.
S2	Der skal benyttes en af kommunen stillet til rådighed VPN-løsning eller anden sikkerhedsteknologi, der tilgodeser krav til autentifikation af brugeren og kryptering af data til at tilgå kommunens systemer og ressourcer via arbejds-PC fra eksterne netværk.	Anbefalingen er opfyldt, hvis 1) der anvendes Always On VPN eller anden sikkerhedsteknologi, når klienten er koblet på netværk uden for kommunens egen it-infrastruktur og 2) Always On VPN eller anden sikkerhedsteknologi forbindes til kommunens egen it-infrastruktur, således at al internettrafik går via kommunen. Tidsbegrænset lokal netværksadgang kan tillades for at kunne anvende login-portaler på fremmed WiFi.
S3	Fysiske klienters harddiske skal krypteres.	Anbefalingen er opfyldt, hvis der er aktiveret fuld diskkryptering af det lokale faste lager på alle klienter i kommunen, typisk vha. indbygget funktionalitet i operativsystemet.
S4	Der skal implementeres endpoint-beskyttelse på klienter.	Anbefalingen er opfyldt, hvis der er installeret endpoint-beskyttelse med automatisk opdatering på alle klienter hos kommunen.
S5	Klienters OS og applikationer på klienten skal holdes sikkerhedsopdateret.	Anbefalingen er opfyldt, hvis: 1) det anvendte operativsystem og applikationerne på klienten er under aktiv support (dvs. at der udgives sikkerhedsopdatering, som adresserer kendte sårbarheder) og 2) der er indført tekniske og/eller organisatoriske foranstaltninger, der sikrer at ikke kritiske systemer opdateres inden for 30 dage, og at kritiske systemer opdateres hurtigst muligt inden da.

S6	Almindelige brugerkonti må ikke tildeles administrative rettigheder til klienter.	Anbefalingen er opfyldt, hvis 1) der er truffet organisatoriske foranstaltninger, med evt. teknisk understøttelse, der sikrer, at administrative rettigheder på klienterne tildeles en separat konto, der kun anvendes til aktiviteter, hvor den administrative rettighed er påkrævet og 2) medarbejdere, hvis primære jobfunktion ikke inkluderer administration af klienter, kun tildels en separat konto med administrative rettigheder i en tidsbegrænset periode, og på baggrund af en dokumenteret godkendelse af et konkret behov. Ved fornyelse skal en ny godkendelse foretages og dokumenteres. Softwarebaseret elevering af brugerens privilegier kan tillades, såfremt det teknisk er sikret, at det kun er den anmodede og godkendte aktivitet, der udføres med de eleverede privilegier. Administratorprivilegier skal således automatisk trækkes tilbage, når den pågældende aktivitet er udført. Brugerens øvrige aktiviteter, som fx mail- og internetbrug, skal fortsat udføres under brugernes almindlige brugerkonto uden specielle privilegier.
S7	Klienter skal anvende det nyeste operativsystem.	Anbefalingen er opfyldt, hvis det anvendte operativsystem (OS) er en major release eller major update udgivet for mindre end 18 måneder siden.
K1	For borger-PC'er gælder det, at tilslutning af eget udstyr skal blokeres fysisk og med krav om administratortilladelse.	Anbefalingen er opfyldt, hvis 1) det er umuligt at tilsluttet eksternt udstyr til PC'er og 2) installation af programmer eller andre ændringer på pc'er kræver administratoradgang
K2	Der skal opsættes en politik for konfiguration af PC'er uden password (fx borger-PC'er), som tilgodeser brugernes sikkerhed i størst muligt omfang.	Anbefalingen er opfyldt, hvis der findes en politik for konfigurering, der 1) beskriver en fysisk sikret tynd klient, med et sikret OS, hvis virtuelle maskine nulstilles efter hver session og 2) at politikken er implementeret på alle PC'er i borgervendte funktioner i kommunen
Nr.	Mail: Anbefalingerne angår mailkommunikation til og fra kommunen.	
S8	Der må kun anvendes godkendte mail-relays med autentifikation.	Anbefalingen er opfyldt, hvis mail-relays, som tilhører eller anvendes af kommunen, kun accepterer mails fra autentificerede brugere eller systemer. Hvor autentifikation ikke understøttes, skal mail kun accepteres fra positvlistede systemer/software.
S9	Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2.	Anbefalingen er opfyldt, hvis 1) alle mail-servere, hvorigennem der kommunikeres til og fra kommunen er sat op til at kryptere mails med TLS 1.2, såfremt modtager understøtter det (opportunistisk TLS) og 2) alle relevante servere er sat op til at foretage tvungen kryptering (forced TLS) til statslige myndigheder og 3) TLS er konfigureret i henhold til De Tekniske minimumskrav for statslige myndigheder 2024 bilag 1: https://www.sikkerdigital.dk/Media/638638815823835221/De%20tekniske%20minimumskrav%20oktober%202024.pdf
S10	Afsenders DMARC-politik skal overholdes ved modtagelse.	Anbefalingen er opfyldt, hvis det sikres, at indgående mailgateways respekterer afsenderdomænets DMARC-politik, såfremt en sådan politik er publiceret af domæneejeren.

Nr.	Autentifikation: Anbefalingerne angår de it-systemer, der kan tilgås fra internettet, og hvor der logges på med kommunens brugerkonti.	
S11	Autentifikation til kommunens systemer over internettet skal anvende flerfaktor-autentificering.	Anbefalingen er opfyldt, hvis 1) flerfaktor-autentifikation er påkrævet ved adgang til de af kommunens it-systemer, som kan tilgås fra internettet og 2) flerfaktor autentifikationen er baseret på brugerens brugernavn og to eller flere autentifikationstyper og 3) såfremt der identificeres på baggrund af en enhed eller biometri, skal brugerens identitet bekræftes og 4) såfremt der anvendes engangskoder skal disse koder genereres lokalt (på enheden) og må ikke transmitteres til brugeren, fx via SMS eller mail.
K3	Alle platforme, hvor man logger på med kommunens legitimationsoplysninger (credentials) må kun anvendes udenfor kommunens lokale netværk, hvis dette foregår vha tofaktor eller via en krypteret forbindelse (VPN, HTTPS el. tilsvarende) til kommunens netværk.	Anbefalingen er opfyldt, hvis 1) der sikres en direkte og krypteret forbindelse ind i kommunens eget netværk via VPN, HTTPS eller lign. - AllwaysON VPN er at foretrække eller 2) der logges ind via 2 faktor login
Nr.	Password: Anbefalingerne angår alle kommunens brugerkonti, herunder konti udstedt til administratorer, it-systemer og services i centrale.	
S12	kommunen skal sikre, at der ikke anvendes tidligere lækkede passwords.	Anbefalingen er opfyldt, hvis 1) der minimum én gang om måneden tjekkes op mod en liste over lækkede passwords og 2) brugerkonti, hvor der anvendes lækkede passwords, tvinges til at skifte password ved næste log-on og 3) kontoejere for it-systemer og servicekonti, der anvender lækkede passwords, orienteres med henblik på skift af password.
K9	Passwords skal udformes, opdateres og opbevares i overensstemmelse med CFCS anbefalinger.	Anbefalingen er opfyldt, hvis de 5 anbefalinger på side 5 i vejledning fra CFCS fra oktober 2023 følges.
Nr.	Mobile enheder: Kravene angår mobiltelefoner og tablets med app-baseret adgang til kommunens data.	
S13	Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation.	Anbefalingen er opfyldt, hvis der anvendes numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation for at få adgang til den mobile enhed.

S14	MDM (Mobile Device Management) skal implementeres på alle mobile enheder.	Anbefalingen er opfyldt, hvis MDM-løsningen 1) sikrer, at de apps der må tilgå kommunens data, leveres som 'managed apps' og 2) sikrer, at kommunens data holdes adskilt fra øvrige data og 3) er i stand til at slette kommunens data på enheden i tilfælde af bortkomst og 4) sletter kommunens data automatisk ved maksimalt 10 fejlslagne loginforsøg og 5) afviser mobile enheder, der er rooted/jailbroken og 6) mobile enheder (telefoner, tablets mv.) er krypterede som CFCS nævner i deres pjece "Mobilsikkerhed" og 7) skærmen låses automatisk efter nogle minutters inaktivitet og 8) notifikationer fra på de applikationer, der kan indeholde følsomme oplysninger fra kommunen, vises i en form så det alene er tydeligt at der er en notifikation, eller helt slås fra
S15	Operativsystem og apps på mobile enheder skal holdes sikkerhedsopdateret	Anbefalingen er opfyldt, hvis 1) operativsystemet er under aktiv support (dvs. at der udgives sikkerhedsopdateringer) og 2) seneste sikkerhedsopdateringer for operativsystem og 'managed apps' er installeret senest 30 dage efter udgivelse og 3) den mobile enhed er sat op til automatisk opdatering af alle installerede apps.
Nr.	Logning: Kravene angår alle internetvendte tjenester og centrale interne it-systemer.	
S16	Der skal aktivt tages stilling til logning, log på alle systemer og tjenester på netværksservere i henhold til kommunens risikovurdering og best practice på området. Der stilles samme krav til eksterne leverandører.	Anbefalingen er opfyldt, hvis 1) logning er implementeret på alle internetvendte tjenester og centrale interne it-systemer jævnfør De Tekniske minimumskrav for statslige myndigheder 2024 bilag 1: https://www.sikkerdigital.dk/Media/638638815823835221/De%20tekniske%20minimumskrav%20oktober%202024.pdf 2) alle logs anvender en fælles tidskilde og samme tidszone og 3) logs er sat til opbevaring i minimum 12 måneder medmindre lovgivning på området tilsiger andet.
Nr.	Domæner: Kravene angår kommunens egne domæner og sikring i forbindelsen med kommunens navneforespørgsler.	
S17	Internetvendte tjenester tilhørende kommunen skal registreres under .dk-domæner.	Anbefalingen er opfyldt, hvis 1) alle internetvendte tjenester tilhørende kommunen er registreret under .dk-domæner, og 2) såfremt kommunen ejer domæner under andre Top-level-domains (TLD's), skal trafik omdirigeres til .dk-domænet. Det er tilladt at anvende andre TLD's uden omdirigering, hvis indholdet på disse tjenester primært er målrettet borgere, myndigheder og virksomheder uden for Danmark.
S18	DNSSEC skal tilknyttes alle domænenavne tilhørende kommunen.	Anbefalingen er opfyldt, hvis alle kommunens domæner er DNSSEC-signerede.
S19	Det skal sikres, at indgående mailgateways ligger i DNSSEC-signerede domæner.	Anbefalingen er opfyldt, hvis alle indgående mailgateways, der håndterer mails for kommunen, ligger i DNSSEC-signerede domnæner.
S20	Der skal anvendes DANE for alle indgående mailgateways.	Anbefalingen er opfyldt, hvis kommunen har publiceret gyldige TLSA-records for alle indgående mailgateways i domæner, der kan modtage mails.

S21	Der skal foretages DNSSEC-validering på svar på navneopslag.	Anbefalingen er opfyldt, hvis alle svar på navneopslag DNSSEC-valideres.
S22	Kommunen skal anvende en sikker DNS-tjeneste eller implementere anden løsning til beskyttelse mod skadelige domæner.	Anbefalingen er opfyldt, hvis 1) kommunen anvender en Sikker DNS-tjeneste, eller der er implementeret en anden løsning, som yder tilsvarende beskyttelse mod skadelige domæner og 2) løsningen er baseret på vedligeholdte negativlister, der opdateres automatisk.
S23	DMARC REJECT policy implementeres på alle domæner tilhørende kommunen.	Anbefalingen er opfyldt, hvis 1) DMARC er implementeret på alle kommunens domæner og 2) DMARC politikken er sat til REJECT på alle kommunens domæner og 3) SPF (Sender Policy Framework) og DKIM (DomainKeys Identified Mail) er implementeret på alle kommunens domæner.
Nr.	Netværk: Kravene angår kommunens trådede og trådløse netværk.	
S24	WIFI på kommunens arbejdsnetværk skal være krypteret med minimum WPA2.	Anbefalingen er opfyldt, hvis adgang til kommunens WiFi-netværk er krypteret med minimum WPA2.
S25	Gæstenetværk skal holdes adskilt fra kommunens interne netværk	Anbefalingen er opfyldt, hvis 1) gæstenetværket er logisk adskilt fra de interne netværk og 2) al trafik fra gæstenetværket betragtes og behandles som trafik fra internettet og 3) udgående trafik fra gæstenetværket skal anvende en anden IP-adresse end trafik fra kommunens interne netværk.
K6	Al netværksadgang skal være behørigt segmenteret.	Anbefalingen er opfyldt, hvis 1) interne netværk på åbne rådhuse, skole og institutioner er logisk adskilt fra de interne netværk og 2) al trafik fra sådanne interne netværk betragtes og behandles som trafik fra internettet og 3) udgående trafik fra sådanne netværk skal anvende en anden IP-adresse end trafik fra kommunens interne netværk.
Nr.	Internetvendte tjenester: Kravene angår de af kommunens it-systemer, der tilgås fra nettet.	
S26	Software på kommunens internetvendte tjenester skal holdes sikkerhedsopdateret	Anbefalingen er opfyldt, hvis 1) det anvendte software og eventuelle tredjepartsbiblioteker på internetvendte systemer, er under aktiv support (dvs. at der udgives sikkerhedsopdateringer, som adresser kendte sårbarheder) og 2) der er indført tekniske og/eller organisatoriske foranstaltninger, der sikrer, at ikke-kritiske systemer sikkerhedsopdateres inden for 30 dage, og at kritiske systemer sikkerhedsopdateres hurtigst muligt inden da.
S27	Adgang til kommunens internetvendte tjenester skal ske over en krypteret forbindelse.	Anbefalingen er opfyldt, hvis alle kommunens internetvendte tjenester kun kan anvendes over en krypteret forbindelse, herunder at: a) HTTP-tilgængelige tjenester automatisk omdirigerer til en HTTPS forbindelse og b) HTTPS-baserede tjenester kun understøtter TLS 1.2 eller højere og c) TLS-krypterede forbindelser er baseret på konfigurationsparametrene jævnfør De Tekniske minimumskrav for statslige myndigheder 2024 bilag 1: https://www.sikkerdigital.dk/Media/638638815823835221/De%20tekniske%20minimumskrav%20oktober%202024.pdf

S28	Internettilgængelige IP-adresser, som kommunen har brugsret over, skal scannes for tjenester.	Anbefalingen er opfyldt, hvis 1) der mindst én gang i kvartalet foretages en scanning af myndighedsejede internettilgængelige IP-adresser for internetvendte tjenester og 2) IP-rangen scannes for alle porte (1-65.535).
Nr.	Interne it-systemer: Kravene angår specifikke interne infrastruktur-enheder og tjenester.	
S29	Software på specifikke interne infrastruktur-enheder og -tjenester skal holdes sikkerhedsopdateret.	Anbefalingen er opfyldt, hvis der er indført tekniske og/eller organisatoriske foranstaltninger, der sikrer, at omfattede infrastruktur-enheder og -tjenester sikkerhedsopdateres inden for 90 dage jævnfør De Tekniske minimumskrav for statslige myndigheder 2024 bilag 1: https://www.sikkerdigital.dk/Media/638638815823835221/De%20tekniske%20minimumskrav%20oktober%202024.pdf
Nr.	Diverse: Kravene falder udenfor de ovenstående katagorier.	
K4	Der skal være adgangskontrol for fysisk adgang til rum med følsomme oplysninger eller udstyr såsom servere, netværksudstyr, der håndterer intern trafik mv.	Anbefalingen er opfyldt, når der er etableret adgangskontrol til rum og/eller udstyr, der kan indeholde følsomme oplysninger, ex. Serverrum, netværksudstyr, arkivrum, printerrum (med mindre follow me print benyttes) og rum, hvor der kan findes følsomme papirer.
K5	Ekstern adgang til eksempelvis konsulenter skal tildeles tidsbegrænset og kun til og med opgavens ophør. Den eksterne adgang skal kun inkludere adgang til relevante systemer/services ift. den konkrete opgaveløsning.	Anbefalingen er opfyldt, hvis 1) der er truffet organisatoriske foranstaltninger, med evt. teknisk understøttelse, der sikrer, at eksterne brugere kun tildeles adgang til relevante systemer/services ift. den konkrete opgaveløsning og 2) adgangen kun gælder i den aktuelle tidsbegrænsede periode den eksterne bruger er godkendt til og 3) ved fornyelse af adgang skal en ny godkendelse foretages og dokumenteres.
K7	Videokameraer skal være beskyttet med ikke-default password og skal være koblet på et sikkert netværk med adgangsbegrænsning.	Anbefalingen er opfyldt, hvis 1) adgang til videooptagelser er velafgrænset gennem bruger/password på videokameraer samt optagelser 2) videokameraer er placeret, så det tilstræbes at mulighed for fysisk manipulation af kameraerne kan forhindres ligesom fysisk placering af eventuelle visningsskærme skal overvejes med henblik på, hvem der kan se dem.
K8	Internet-of-Things enheder skal være beskyttet med ikke-default password og skal være koblet på et behørigt segmenteret netværk.	Anbefalingen er opfyldt, hvis 1) adgang til Internet-of-things enheder er velafgrænset gennem bruger/password og 2)Internet-of-things enhederne er koblet på et segmenteret net 3) øvrige anbefalinger i vejledningen fra CFCS side 5 følges
K9	Der skal tages backup af vigtige data og systemkonfigurationer.	Anbefalingen er opfyldt, hvis 1) der findes en godkendt backuppolitik og 2) backuppolitikken testes regelmæssigt og 3) beskyttes mod manipulation af eksempelvis ransomwareaktører.
K10	Hjemmesider bør sikres mod angrebsteknikker i OWASP Top 10.	Anbefalingen er opfyldt, hvis inernetvendte services og hjemmesider testes imod den til enhver tid gældende version af OWASP top 10 listen.
K11	Alle hjemmesider og internetvendte services bør kun sikres via HTTPS headers	Anbefalingen er opfyldt, hvis 1) Strict-Transport-Security-headeren er tilføjet i alle kommunens webserversvar og 2) det sikres at brugere kun tilgår HTTPS-beskyttede hjemmesider med HTTPS, uden at forlade sig på redirection fra HTTP.