AUGUST 2025

Informationssikkerhed

Anbefalinger for selvejende institutioner på voksen- og ungdoms-uddannelsesområdet

FRA
LEDERNETVÆRK OM INFORMATIONSSIKKERHED
FOR SELVEJENDE INSTITUTIONER (LISSI)

LISSI ER ET INSTITUTIONSSAMARBEJDE FACILITERET AF
STYRELSEN FOR IT OG LÆRING,
BØRNE- OG UNDERVISNINGSMINISTERIET

INDLEDNING

Det er blevet farligere at være online. Flere hackerangreb inden for det seneste år har demonstreret, at den danske uddannelsessektor ikke er forskånet, og at prisen for utilstrækkelig beskyttelse er meget høj.

På den baggrund er der brug for at tale om tilpasninger i den måde, uddannelsesinstitutionerne bruger it på. Behovet for øget sikkerhed kommer til at gribe ind i hverdagen, men det kan stadig spille sammen med – ikke imod – udviklingen af it som et pædagogisk instrument. For at få det til at lykkes, er det imidlertid afgørende, at ledelsen engagerer sig aktivt og konstruktivt i de diskussioner.

Anbefalingerne her er rettet til skoleledelserne, ikke til it-afdelingerne. De er tænkt som et afsæt til at tage diskussioner med pædagogisk og administrativt personale såvel som bestyrelsen. Anbefalingerne handler i første omgang om, hvordan skolen kan overveje og afveje forskellige hensyn og få dem indarbejdet i sin it-politik. Grundidéen er, at sikkerhed mestendels handler om de generelle it-valg, skolen foretager, og de rammer, som ledelsen sætter for it-brug – ikke et ekstra produkt, der tilkøbes bagefter.

De henviser dog også til meget konkrete sikkerhedsforanstaltninger, som skolen kan tale med it-afdelingen, -fællesskabet eller -leverandører om. Disse tiltag baserer sig på de tekniske minimumskrav til statslige myndigheder, som er udarbejdet af CFCS, Digitaliseringsstyrelsen, m.fl.

En skole er ikke en statslig myndighed, og det er usandsynligt, at nogen skole vil kunne leve op til alle kravene. Givet den trussel, vi står over for, er det dog blevet relevant at genbesøge og evaluere it-sikkerheden, og kravene er en god målestok. Tal med jeres it-leverandør/-afdeling om hvilke af disse sikkerhedstiltag, I allerede efterlever og hvilke, I kan efterleve med nogle af de kursjusteringer, vi slår til lyd for her. I kan finde hjælp til at prioritere indsatsen i.f.t. det tekniske i bilag 1.

LEDERNETVÆRK OM INFORMATIONSSIKKERHED FOR SELVEJENDE INSTITUTIONER

Anbefalingerne er blevet udfærdiget af en arbejdsgruppe under Ledernetværk om Informationssikkerhed på Selvejende Institutioner (LISSI).

Ledernetværket er nedsat og sekretariatsbetjenes af Styrelsen for It og Læring (STIL). Med LISSI er der skabt et forum for udveksling af "best practice" og dialog om udfordringer, både skole-til-skole og imellem sektoren og STIL. Ledernetværket består af 12 medlemmer, som rekrutteres med henblik på en bred repræsentation af det selvejende voksen- og ungdomsuddannelses-område og indsigt i informationssikkerhed og databeskyttelse. Medlemmerne udpeges af STIL i samråd med lederforeningerne på voksen- og ungdomsuddannelsesområdet.

Medlemmer:

- Bjarne Grevsen Thams, Rektor, Solrød Gymnasium
- Ivan Sommer, DPO, FGU Danmark
- Jesper Eriksen, It- og Kommunikationschef, TietgenSkolen
- Jonas Makram Benzarti, Uddannelses- og databeskyttelseskonsulent, Danske Gymnasier
- Lars Levin, It-leder, Social- og Sundhedsskolen Fyn
- Martin Ingemann, Rektor, Egaa Gymnasium
- Mik Helmich, It-chef, KVUC
- Palle Grønbæk, DPO, Nordjyske gymnasier
- Rune Gråbæk, tidl. It- og Digitaliseringschef, ZBC (udtrådt 31/07/2025)
- Tage Oskar Petersen, Direktør, It-center Nord
- Thomas Friis Poulsen, CISO/CTO, EFIF
- Trine Simmel Olsen, Økonomikonsulent, Danske Erhvervsskoler og -Gymnasier

Dennis Quinones Rodriguez, Bagsværd Kostskole og Gymnasium, og Per Andersen, TietgenSkolen, har bidraget til udarbejdelsen af anbefalingerne.

Ledernetværket identificerer selv problematikker på tværs af institutionernes uddannelses-områder, som der med fordel kan arbejdes med i fællesskab. Holdningerne udtrykt i dokumen-tet repræsenterer ikke nødvendigvis Børne- og Undervisningsministeriets eller STILs vurderinger eller holdninger eller de deltagende lederforeningers vurderinger eller holdninger.

Du kan læse mere om LISSI på STILs hjemmeside.

1. UDARBEJD RETNINGSLINJER FOR VALG AF PÆDAGOGISKE IT-LØSNINGER

Vi har opgjort på en teknisk skole, at de havde 7000 applikationer. Hvis vi skulle opdatere alle de applikationer, skulle vi være mange flere end vi er.
– Tage, ITCN

Der er ingen knaphed på pædagogiske it-løsninger. Enhver med adgang til internettet kan i princippet hente applikationer. Enhver med adgang til en udgiftskonto kan i princippet købe smarte dimser.

Både applikationer og dimser er imidlertid små tidsindstillede bomber under jeres sikkerhed. Ingenting i it forbliver sikkert uden sikkerhedsopdateringer. Hvis en medarbejder har fundet og installeret en applikation – eller opfordret eleverne til at installere den – hvem tjekker så, at leverandøren har planer om sikkerhedsopdateringer? Og hvis der kommer sikkerheds-opdateringer, hvem sørger så for, at de bliver implementeret? Hvem har overblikket over de løsninger, der bruges på skolens maskiner?

Internettets overflod skabte ræsonnementet, at hvis noget var gratis, behøvede man ikke at spørge om lov. I it-sikkerhedssammenhæng er prisen irrelevant.

I praksis er det uholdbart at sikre skolens computere, telefoner og anden it, hvis hver medarbejder selv styrer valget af løsninger egenhændigt. Hvis medarbejderen tillige har administrator-rettigheder på maskinen, bliver det umuligt. Heldigvis kan man kan godt have metodefrihed uden at have uindskrænket råderet over sin PC eller mobil – eller frit valg på alle internettets hylder.

LEDELSESMÆSSIGE ANBEFALINGER

- **Spørg jer selv:** Har I brug for ti forskellige quiz-programmer eller kan I finde ét, alle kan leve med? Hvem har egentlig brug for administrator-rettigheder på arbejds-pc'en?
- **Proces:** Tal med undervisere, vejledere og it. Hvordan forstår de metodefrihed inden for rammerne af pædagogisk it – og hvordan kan det forlenes med it-sikkerhed?
- **It-politik:** Valg af it-løsninger er noget, I foretager i fællesskab, ikke individuelt. Det flugter også godt med principper om en fælles pædagogisk-didaktisk tilgang.
- **Retningslinjer:** Hvordan foretager I valget helt konkret? Sørg for at inddrage it, pædagogisk ledelse og personale. Overvej om uddannelser med særlige behov kan køre på særskilte løsninger fremfor at sætte niveauet for alle.

TEKNISKE ANBEFALINGER (FRA DE TEKNISKE MINIMUMSKRAV , OKTOBER 2024)

- **Krav 5:** Klienters OS og applikationer på klienten skal holdes sikkerhedsopdateret.
- **Krav 6:** Almindelige brugerkonti må ikke tildeles administrative rettigheder til klienter.

Terminologi:

- klient: en laptop eller desktop computer (uanset om den kører Windows, MacOS, linux el.a.)
- administrative rettigheder: Rettigheder, der går ud over den normale brugers rettigheder, normalt forbeholdt it-administratoren. Kræves f.eks. til installation af software på klienten.

Se bilag 1 for mere om de tekniske anbefalinger.

2. SÆT KLARE RAMMER FOR PRIVATBRUG AF UDLEVERET IT-UDSTYR

En laptop, tablet, mobiltelefon eller anden it, der udleveres til medarbejdere til arbejdsbrug, kan også anvendes privat. Det risikerer imidlertid at forværre problemerne nævnt under det sidste afsnit. It kan ikke sørge for, at spil, fitnessprogrammer m.m. er sikkert at bruge eller opdateret. Hvis skolens it-kultur lægger op til, at arbejds-it også er til privat brug, skabes der nye sårbarheder og lægges beslag på knappe ressourcer.

Og det er ikke kun medarbejderressourcer. Under corona introducerede mange skoler VPN-adgang ved hjemmearbejde. En VPN bidrager til sikkerheden (se ”Relevante anbefalinger…” på næste side) og indgår i anbefalingerne. Privat streaming- og spillebrug derhjemme kan imidlertid gøre det dyrere at implementere en VPN-løsning, fordi trafikken bruger af skolens begrænsede båndbredde.

En udbredt indstilling har været, at så længe privat brug ikke forekommer i arbejdstiden, koster det ikke skolen noget. Trusselsniveauet, vi ser i dag, bør lede til at genoverveje den tankegang.

LEDELSESMÆSSIGE ANBEFALINGER

- **Spørg jer selv:** Har I italesat, hvad skolens it er beregnet til og må bruges til? Eller er I bare nået frem til en praksis baseret på uudtalte forventninger?
- **Proces:** Tal med personalet om, hvad deres forventninger er. Vurdér om I er parate til et opgør med privat-brugs-praksis, hvis I har sådan en.
- **It-politik:** Udleveret it er til arbejdsbrug.
- **Retningslinjer:** Uddyb politikken. Eks. privat opslag på nettet eller regnskab i regneark er ok; programmer, spil, streaming og træk på support er ikke.

TEKNISKE ANBEFALINGER (FRA DE TEKNISKE MINIMUMSKRAV, OKTOBER 2024)

- **Krav 2:** Klienter skal benytte Always On VPN fra eksterne netværk.
- **Krav 5:** Klienters OS og applikationer på klienten skal holdes sikkerhedsopdateret.
- **Krav 6:** Almindelige brugerkonti må ikke tildeles administrative rettigheder til klienter.

Terminologi:

- VPN: Virtual Privat Network. Sikker adgang fra hjemmearbejde til skolens netværk.

Se bilag 1 for mere om de tekniske anbefalinger.

3. SKAB ET POSITIVT NARRATIV OMKRING INFORMATIONSSIKKERHED

Men hvis der går et stykke tid inden medarbejderen accepterer en sikkerhedsopdatering, så bliver den gennemtvunget fra Microsoft. Så genstarter computeren og går i gang med installationen. Og så kan de stå midt i undervisningen…
– Tage, ITCN

Hvorfor er det, at man har de her begrænsninger? Årsagen er jo ikke, at vi vil irritere folk, at vi vil gøre livet svært for dem. Årsagen er jo, at vi vil beskytte nogle data, og dermed også beskytte nogle mennesker.
– Ivan, FGU Danmark

Ubelejlige sikkerhedsopdateringer. Multi-faktor-autentifikation, der kræver telefon op af lommen for at give adgang. Forbud imod passwordgenbrug. At skulle gå rundt med to telefoner, én til arbejde og én privat.

It-sikkerhedsforanstaltninger opleves ofte som noget bøvl. Underviserne kan let komme til at opleve, at det er bøvl, som tager tid og opmærksomhed fra undervisningen. Det kan skabe en følelse af konflikt – at du enten kan få god undervisning eller god sikkerhed, men ikke begge dele.

Det er en forståelig, men falsk modsætning. Nogle skoler har oplevet, at sikkerheden svigtede så meget, at de blev hacket, at alle deres systemer blev utilgængelige, og at undervisnings-materialer forsvandt. Når man står i den situation, er hverdagen meget mere bøvlet end at skulle huske 15 tegn.

It-sikkerhed er en forudsætning for en god skoledag, ikke dens fjende. Ledelsen har en vigtig rolle med at hjælpe med at italesætte det og sætte det gode eksempel.

LEDELSESMÆSSIGE ANBEFALINGER

- **Spørg jer selv:** Hvordan taler I om it-sikkerhed på skolen? Som bøvl eller som bidrag?
- **Proces:** Tal om det, der opleves som fnidder i dagligdagen. Afsøg med it, om der er måder at afbøde tidstab o.lign. uden at anfægte det saglige sikkerhedshensyn.
- **It-politik:** Regelmæssige fælles awareness-tiltag, gerne med afsæt i lokale erfaringer, der giver forståelse for, hvad it-sikkerhedsforanstaltningerne er til for.
- **Retningslinie:** (eks.) Prioritér sikkerhedsopdateringer – det er (også) en del af arbejdet.

TEKNISKE ANBEFALINGER (FRA DE TEKNISKE MINIMUMSKRAV, OKTOBER 2024)

- **Krav 7:** Klienter skal anvende det nyeste operativsystem.
- **Krav 11:** Autentifikation til […] systemer over internettet skal anvende flerfaktor-autentificering (MFA).
- **Krav 12:** […] sikre, at der ikke anvendes tidligere lækkede passwords.
- **Krav 14:** MDM (Mobile Device Management) skal implementeres på alle mobile enheder.

Terminologi:

- MDM: Central styring af mobiltelefoner. Kan sætte restriktioner på installérbare apps, beskytte udvalgte informationer på telefonen og implementere fjernstyret sletning af data.
- MFA: Dét at bruge flere elementer til at autentificere sig selv, dvs. bevise, at man er den, man siger, at man er. Et password er én faktor. Biometri (fingeraftryk, ansigtsgenkendelse) kan være en anden. At bevise, at man er i besiddelse af en telefon kan også være en faktor.

Se bilag 1 for mere om de tekniske anbefalinger.

4. FIND DEN RETTE BALANCE MELLEM ÅBEN ADGANG OG SIKKER DRIFT

En uddannelsesinstitution tager konstant nye mennesker ind. Nye elever, nye fastansatte, nye midlertidige og vikarer, nye samarbejdspartnere. Skolen kan ønske at fremstå så åben som muligt for ikke at opstille barrierer for udefrakommende. Det er en udfordring for it-sikkerhed, der traditionelt forudsætter klare grænser imellem det indre og det ydre.

Et wifi-netværk, der ikke kræver login, er let for nytilkomne at hoppe på. Det er dog usikkert for både skolen og alle andre på netværket. Ét fælles netværk for alle – medarbejdere, elever, gæster – er nemmest og mest åbent, men risikerer at give uvedkommende adgang til ressourcer, de ikke bør have adgang til.

En timelærer på udlån fra naboskolen eller en lokal virksomhed vil have meget lettere ved at starte op, hvis de kan bruge egen privat eller hjemmeskole-laptop fremfor at skulle anvende en separat PC kun for sit arbejde for jeres skole. Hvis 'udefrakommende' maskiner får adgang til jeres interne netværksressourcer, skal I kunne stole på, at de er tilstrækkeligt beskyttede. At basere sig på ren tillid er ikke god it-sikkerhed. Det samme gælder for medarbejdere, der måtte ønske at bruge private devices til arbejdsbrug.

Det er vigtigt at fremstå som en tilnærmelig, åben og attraktiv organisation for ansatte og samarbejdspartnere. Det bør dog afvejes imod hensynet til skolens sikkerhed.

LEDELSESMÆSSIGE ANBEFALINGER

- **Spørg jer selv:** Hvem er på jeres netværk? Har I kontrol over de maskiner, der tilgår jeres data? Er maskiner, I ikke kontrollerer, på et separat, udskilt netværk?
- **Proces:** Tal med it og medarbejdere samarbejdspartnere, der har én fod på skolen og én udenfor. Find løsninger, der ikke baserer sig på blind tillid til deres devices.
- **It-politik:** Hvis en maskine skal have adgang til skolens interne it-systemer, skal den være under skolens administration.

TEKNISKE ANBEFALINGER (FRA DE TEKNISKE MINIMUMSKRAV, OKTOBER 2024)

- **Krav 1:** Der skal implementeres firewall på klienterne.
- **Krav 4:** Der skal implementeres endpoint-beskyttelse på klienter.
- **Krav 24:** […] WiFi-netværk skal være krypteret med minimum WPA2.
- **Krav 25:** Gæstenetværk skal holdes adskilt fra […] interne netværk.

Terminologi:

- firewall: En kontrol, der regulerer netværkstrafik ind og ud af maskinen. Trafik kan tillades eller blokeres.
- endpoint-beskyttelse: En fællesbetegnelse for antivirus o.a. tiltag, der beskytter en klient (PC m.m.) imod malware.

Se bilag 1 for mere om de tekniske anbefalinger.

BILAG 1: TJEK JERES SIKKERHEDSNIVEAU UD FRA DE TEKNISKE MINIMUMSKRAV

De tekniske minimumskrav er it-sikkerhedskrav, som alle statslige myndigheder (ministerier, styrelser o.lign.) skal leve op til. De blev introduceret i 2020 og opdateret løbende siden. Nogle er lettere at leve op til end andre; nogle vil være mere relevante for en uddannelsesinstitution end andre. Fælles for dem er, at deres relevans og effektivitet for it-sikkerhed er gennemtænkt og gennemarbejdet af stærke kompetencer fra bl.a. CFCS, Digitaliseringsstyrelsen m.fl. Hvis I efterlever nedenstående, er I godt på vej i.f.t. den tekniske side af sagen.

I nedenstående skema kan I finde en kort oversigt over de allermest relevante af minimums-kravene for institutionernes udfordringer. Vi anbefaler, at I tjekker den fulde liste på sikkerdigital.dk og gennemgår den med jeres it-afdeling/-leverandører.

Nr.	Krav	Relevant for…	Udfordring
1	Der skal implementeres firewall på klienterne.	Anbefaling 4	Hvis maskinen ikke er administreret af skolen, er det svært for skolen at vide, om der er en (tilstrækkelig) firewall på den.
2	Klienter skal benytte Always On VPN fra eksterne netværk.	Anbefaling 2	En VPN betyder, at skolens netværk er mellemstation for hjemmearbejde-internettrafik. Privat streaming (fx Netflix) kan trække meget store veksler på netværket til skade for andres arbejdsbrug.
4	Der skal implementeres endpoint-beskyttelse på klienter.	Anbefaling 4	Hvis maskinen ikke er administreret af skolen, er det svært for skolen at vide, om der er (tilstrækkelig) endpoint-beskyttelse på den.
5	Klienters OS og applikationer på klienten skal holdes sikkerheds-opdateret.	Anbefaling 1 og 2	Når hver medarbejder selv henter apps, kan it ikke sørge for sikkerheds-opdateringer eller bevare overblikket.
6	Almindelige brugerkonti må ikke tildeles administrative rettigheder til klienter.	Anbefaling 1 og 2	Hvis medarbejderen har administratorrettigheder for at kunne installere applikationer m.m., giver man malware og hackere let spil.
7	Klienter skal anvende det nyeste operativsystem.	Anbefaling 3	Sikkerhedsopdateringer kommer sjældent belejligt.
11	Autentifikation til […] systemer over internettet skal anvende flerfaktor-autentificering (MFA).	Anbefaling 3	Multi-faktor-autentifikation øger sikkerheden gevaldigt, men tager lige lidt mere tid at gennemføre.

12	[…] sikre, at der ikke anvendes tidligere lækkede passwords.	Anbefaling 3	Lækkede passwords fra et website er et problem, hvis brugerne genbruger passwordet til andre tjenester, f.eks. skolens. Genbrug af passwords er udbredt, da det gør dem nemmere at huske.
14	MDM (Mobile Device Management) skal implementeres på alle mobile enheder.	Anbefaling 3	MDM er let at implementere på arbejdstelefoner, men svært på private telefoner (hvilket også kræver samtykke).
24	[…] WiFi-netværk skal være krypteret med minimum WPA2	Anbefaling 4	Hvis skolen kører med et åbent netværk (uden kryptering), er det svært at kontrollere hvem, der er på netværket samt forebygge aflytning.
25	Gæstenetværk skal holdes adskilt fra […] interne netværk	Anbefaling 4	Gæster har som udgangspunkt ikke behov for at tilgå de samme ressourcer som medarbejdere. Det er god sikkerheds-hygiejne, at de opererer på et separat netværk. Det problematiseres dog, hvis der ikke er en klar skelnen imellem hvem, der er medarbejder, og hvem, der er gæst.