VALGdirektoratet

Veileder i sikkerhet

Hvordan gjennomføre sikre valg i kommuner og fylkeskommuner

Versjon 4
25. juni 2025

Endringslogg

#	Versjon	Punkt	Dato	Innhold	Hvem
1	2.1.	-	09.03.23		John Andreas Johnsen
2	2.2	5.1	10.03.23		John Andreas Johnsen
3	3.0	-	25.11.24		John Andreas Johnsen
4	3.1	2.3	06.02.25		John Andreas Johnsen
5	4.0	-	25.06.25	Endret ordlyd gjennom veilederen for å gjenspeile valgforskriften § 4-2, spesielt endret kapittel 5	John Andreas Johnsen

1 Innholdsfortegnelse

2 Innledning

Ett av Valgdirektoratets hovedmål er å bidra til en korrekt og sikker valggjennomføring med tillit i befolkningen. Denne sikkerhetsveilederen er ett av våre bidrag til kommunene og fylkeskommunene for å nå dette målet.

I veilederen finner du som valgansvarlig i kommunen eller fylkeskommunen konkrete råd, slik at dere kan få på plass gode tiltak og etablere rutiner knyttet til:

- Sikring av valgmateriell og IKT-utstyr som skal brukes i forbindelse med valggjennomføringen.
- Sikring av lokaler og IKT-utstyr for maskinell opptelling av stemmesedler.
- Sikkerhetstiltak for oppbevaring av IKT-utstyr som skal benyttes.
- Sikring av opptellingslokaler der telling av stemmesedler skal foregå.
- Sikring av valglokalet der stemmegivning utføres.
- Sikker infrastruktur og bruk av EVA-applikasjonene.

Sikkerhetstiltak, enten organisatoriske, menneskelige eller tekniske tar lang tid å implementere. Tiltakene kan også i noen tilfeller medføre kostnader. Valgdirektoratet anbefaler derfor at veilederen gjennomgås i god tid før valggjennomføringen og at tiltakene planlegges og iverksettes, slik at de er effektive under *hele* valggjennomføringen.

Anbefalte sikkerhetstiltak bidrar til å fjerne sårbarheter og redusere risiko. I tillegg styrker tiltakene arbeidet med å:

- Forebygge omdømmetap.
- Opprettholde tilliten til valggjennomføring og valgresultatet.
- Forebygge forsinkelser.
- Forebygge manipulering av valgresultatet.

Vi anbefaler videre at de tekniske tiltakene i kapitlene 5 og 6 leses og planlegges sammen med teknisk personell. Merk at hoveddelen av de tekniske tiltakene også gjelder IKT-utstyr brukt til EVA Admin, ikke bare EVA Skanning.

Betydning av ordlyd i veilederen
Gjennom veilederen benyttes ulik ordlyd, ettersom det hører med et krav hjemlet i regelverket, eller om det er anbefalinger som bør følges. Ordlydene det er snakk om:

- ***Skal*: Tiltaket stammer fra valgloven eller forskrift, og kommunen eller fylkeskommunen er gjennom dette pålagt å følge regelverket.**
- ***Må*: Alternativ ordlyd til *skal*. Følger også av regelverk. Brukes også i enkelte tilfeller om tiltak som må gjøres for å oppfylle Valgdirektoratets anbefalinger. Dette vil i så fall framgå av sammenhengen i teksten.**
- ***Bør*: Tiltaket stammer ikke fra valgloven eller forskrift, men kan følge av Valgdirektoratets anbefalinger eller andre virksomheters anbefalinger – for eksempel NSMs Grunnprinsipper for IKT-sikkerhet. Kommunen eller fylkeskommunen er ikke pålagt å følge tiltak med bør-ordlyd, men oppfordres sterkt til å gjøre det.**
- ***Anbefaling*: Alternativ ordlyd til *bør*. Anbefalinger er ofte knyttet til Valgdirektoratets egne vurderinger og anbefalinger.**

2.1 Sjekkliste for å gjennomføre sikkerhetstiltak

Det er av stor betydning at du som valgansvarlig i kommunene og fylkeskommunene setter deg inn i sikringstiltak og prosedyrer som etableres i kommunen. Gode sikringstiltak kjennetegnes ved at de er hensiktsmessige og praktisk utformet slik at tiltakene blir enkle å følge og oppleves som relevante. Videre må det legges vekt på å oppnå forståelse av tiltakene og at det er gevinster ved å følge veiledningen i form av tillit til valggjennomføringen.

For å bidra til dette, følger det med en sjekkliste som dere kan bruke for å kontrollere at tiltak i denne veilederen innføres. Sjekklisten følger med som vedlegg til veilederen.

2.2 Risiko og sårbarhetsanalyse (ROS)

ROS er et viktig verktøy for å kunne styre risikoen gjennom valggjennomføringen.

Det forutsettes at kommunene gjør en risiko og sårbarhetsanalyse i forkant av valggjennomføringen. En ROS har to formål:

1. Avdekke mulige hendelser, risiko for at disse oppstår, og en vurdering av konsekvensen.
2. Belyse hvilke tiltak som kan iverksettes for å redusere enten *sannsynligheten for*, eller *konsekvensen av* hendelsene.

Når ROS er gjennomført bør valgstyret beslutte om risiko og tiltak er akseptable.

Dette kan for eksempel gjøres ved at valgstyret blir forelagt den fullstendige analysen eller et utdrag og oppsummering gjort av administrasjonen. Vi anbefaler at dere går i dialog med valgstyret om behovet. Dersom risikonivået ikke er akseptabelt, må ytterligere tiltak iverksettes.

Det finnes mange metoder for risikoanalyse og håndtering. Flere kommuner og fylkeskommuner har det allerede i sitt daglige virke. Vi anbefaler at kommunene og fylkeskommunene benytter prosess og metode som allerede er etablert.

For de som ikke har dette i sitt daglige virke, anbefaler vi Digitaliseringsdirektoratet sine veiledere.

Digdir.no – Om risiko og risikovurdering

Du kan finne mer informasjon om risiko, sårbarhet og beredskap på DSB sine sider.

Dsb.no – Risiko, sårbarhet og beredskap

Valgdirektoratet har laget en forenklet mal for Risikovurdering. Malen ligger som vedlegg til veilederen.

2.3 Mer om sikkerhet

Denne veilederen er utarbeidet av Valgdirektoratet og er basert på NSMs publiserte sikkerhetsveiledere og rapporter. For å lese mer om sikkerhet og få tilgang til ytterligere veiledning og informasjon kan du oppsøke NSMs nettsider.

NSM.no

Tiltakene i denne veilederen bør leses som et *minimumsnivå* av sikkerhet ved valg. Flere kommuner har ytterligere sikkerhetstiltak i sin portefølje.

NSM publiserer jevnlig rapporter og veiledere. Flere av disse gir verdi i valggjennomføringen, men kan være omfattende. Rapportene og veilederne fra NSM er relevante både i valggjennomføring og generelt sikkerhetsarbeid i kommunene og fylkeskommunene. Her er en liste over anbefalte veiledere og rapporter publisert av NSM:

- Grunnprinsipper for IKT-sikkerhet versjon 2.1
- Grunnprinsipper for fysisk sikkerhet
- Veileder i sikkerhetsstyring
- Temarapport: Innsiderisiko
- Rapport: Risiko 2025

I tillegg publiserer E-tjenesten og PST årlige åpne trusselvurderinger. Vi anbefaler at kommuner og fylkeskommuner holder seg oppdatert med vurderingene i rapportene under.

- PST: Nasjonal trusselvurdering 2025

- Etterretningstjenesten: Fokus 2025

PST sin årlige åpne trusselvurdering publiseres normalt i februar.

3 Fysisk sikring

Alle kommuner og fylkeskommuner som gjennomfører valg bør tilrettelegge for fysisk sikring av lokaler og utstyr som skal benyttes under valggjennomføringen. Det innebærer å ha gode rutiner for hvem som har tilgang til valgutstyret samt hvordan dette oppbevares og fraktes. Rutiner som har avgjørende betydning for en vellykket valggjennomføring, bør øves og testes i forkant av valget.

Valgstyret skal sørge for at det fastsettes betryggende, skriftlig rutiner for forsegling, oppbevaring og transport av valgmateriell i alle faser av valggjennomføringen, jf. valgforskriften § 9-1 (1) til (3).

Innholdet i dette kapittelet kan anvendes som et utgangspunkt for å etablere betryggende *skriftlige rutiner* for forsegling, oppbevaring og transport av valgmateriell og valgutstyr.

3.1 Soneinndeling

Valgdirektoratet anbefaler kommunene å ta i bruk soneinndeling som verktøy for å kontrollere adgang til ulike områder i valggjennomføringen. Lokalene som benyttes skal da inndeles i henholdsvis grønn og rød sone, og ha ulike krav til sikring.

En hensiktsmessig soneinndeling og kontroll med sonene bidrar til å redusere trusler ved å:

- Redusere antall personer med tilgang til lokaler, valgmateriell og maskinvare.
- Føre kontroll med personer med tilgang til lokalene.
- Bevisstgjøre personell og øke sikkerhetsfokus.

Under følger en nærmere forklaring av hvilke prinsipper som ligger til grunn for sonemodellen, og hvilke tiltak som må gjennomføres for å oppfylle direktoratets anbefalinger.

3.1.1 Grønn sone

En grønn sone er et område som er åpent tilgjengelig for allmennheten, som for eksempel fellesarealer og servicesenter i kommunen og fylkeskommunen. Under valggjennomføringen er dette området der valgavlukker står, og observasjon av opptelling kan foregå.

I grønn sone er det ikke behov for særskilt vakthold eller overvåking. Sonen er ikke begrenset utover generelt oppsyn og åpningstider. Utenom åpningstid bør området være avlåst.

Grønn sone er minimum sikret med:

- Avlåsing utenom åpningstid.

3.1.2 Rød sone

Rød sone er et område som kun er tilgjengelig for personell med tjenstlige behov, for eksempel valgansvarlig, valgmedarbeidere som tar imot stemmer, opptellingspersonell eller IT-personell.

Personellet skal være akkreditert til området definert som rød sone. Tilgang til området skal registreres med informasjon om *hvem* (fullt navn) og *tidspunkt* (dato og klokkeslett fra og til). Det er relevant å registrere tilgang gjennom hele valggjennomføringen. Det kan også eksistere flere røde soner hvor forskjellig personell har tjenstlig behov. Eksempelvis er det ikke alltid nødvendig at personell som tar imot stemmer også har behov for tilgang til sone for opptelling. Akkrediteringen til hver enkelt medarbeider skal definere hvilke røde soner hen har tjenstlig behov for tilgang til.

Den sentrale valgorganisasjonen i kommunen har ansvar for akkreditering av medarbeidere.

Rød sone er minimum sikret med:

- Avlåsing.
    - Avlåsing kan erstattes med vakthold.
- Registrering av alle som entrer og forlater sonen, eksempelvis:
    - Elektroniske dørlåser for automatisk inn- og ut-registrering.
    - Videoovervåking av inn- og ut-registrering.
- Innbrudds- og brannalarm.

Personell som har tjenstlig behov for tilgang til disse områdene under valggjennomføringen, er i hovedsak:

- Valgansvarlige.
- IT-personell.
- Valgmedarbeidere med akkreditering og tildelt rolle i valggjennomføringen, eksempelvis:
    - Personell som jobber med opptelling.
    - Personell som tar imot stemmer.

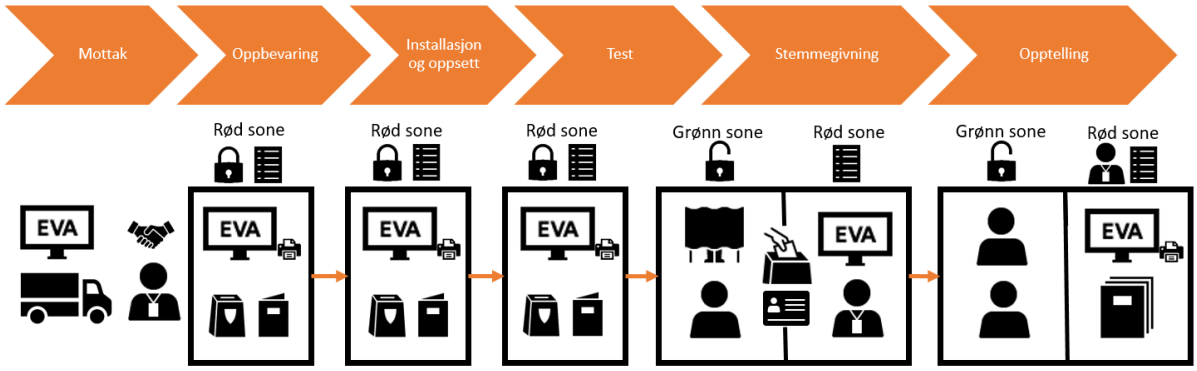
Kommuner og fylkeskommuner som benytter seg av eksterne leverandører, for eksempel en leverandør for skanning av stemmesedler, kan også gi personell fra leverandør tilgang til nødvendige røde soner dersom det er tjenstlig behov.

3.2 Sikring av valgmateriell og IKT-utstyr

Anbefalingene til fysisk sikkerhet er gitt for å sikre maskinvaren og at annet valgmateriell er tilgjengelig når det skal tas i bruk og/eller sikret mot kompromittering ved at uvedkommende har fått urettmessig tilgang. Tiltakene er knyttet til å sikre lokaler der dette materiellet befinner seg. To eksempler på slikt utstyr er PC-er som brukes med EVA Admin og stemmesedler.

Krav til informasjonssikkerhet på PC-ene som brukes i valggjennomføringen er nå forskriftsfestet. Anbefalingene i dette kapittelet er et ytterligere lag med tiltak for å redusere sannsynligheten for at uvedkommende får urettmessig tilgang til utstyr og materiell som benyttes i valggjennomføringen.

Skissen under illustrerer soneinndeling under valggjennomføringen.



Denne kjeden har primært to kritiske hovedelementer:

- Tilgangskontroll for lokaler der materiell oppbevares.
- Flytting eller overgang fra et ledd i leveransekjeden til et annet.

Valgmateriell og maskinvare som skal sikres med rød sone kan ikke bli stående i en sone med lavere nivå uten tilsyn. For eksempel vil man ikke lenger ha kontroll dersom PC-er, eller annet valgmateriell, blir stående uten tilsyn i kommunens servicesenter eller varemottak. Materiellet har da vært tilgjengelig for personell uten tjenstlig behov.

«Maskinvare» defineres som IKT-utstyr som skal benyttes i valggjennomføringen. Dette omfatter blant annet:

- PC-er der EVA-applikasjonene skal brukes.
- Buypass smartkortlesere som skal brukes av EVA-applikasjonene.
- Strekkodeskannere som skal brukes av EVA-applikasjonene.
- Dokumentskannere som skal brukes av EVA Skanning.
- Nettverksutstyr.

3.2.1 Sikring før valggjennomføring

For å begrense hvem som har tilgang til materiellet og maskinvaren i forkant av valget, bør dette oppbevares i rød sone til enhver tid. Dette begrenser muligheter for sabotasje eller andre uønskede hendelser.

Dersom kommunen eller fylkeskommunen benytter maskinvare som også brukes til annet enn valggjennomføring, er det viktig at maskinvaren har vært oppbevart i rød sone, eller er under tilsyn av brukeren som har fått utlevert utstyret.

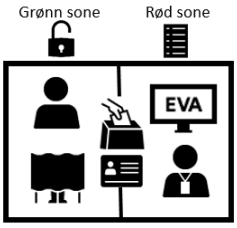
Valgmateriell og maskinvare til bruk i valggjennomføringen bør oppbevares i rød sone fra materiellet ankommer kommunen eller fylkeskommunen, og til valget er gjennomført og godkjent. Kun autorisert personell med særskilt tjenstlig behov skal ha tilgang. Eksempelvis valgansvarlig i kommunen og fylkeskommunen og IKT-personell i valggjennomføringen. Dersom maskinvaren skal brukes igjen ved neste valg, er det viktig at denne fortsatt oppbevares i rød sone etter at valget er over.

Ansatte/valgmedarbeidere som har med utstyr ut av rød sone, for eksempel til bruk i forbindelse med hjemmekontor, skal påse at utstyret er nedlåst i skap/skuff eller i forseglingspose når det ikke er i bruk. Nøkkel og utstyr kan ikke deles med andre (eksempelvis familiemedlemmer) som ikke har tjenstlig behov for tilgang.

Denne sikringen gjelder for følgende lokaler:

- Oppbevaringsrom/lager for materiellet.
- Lokaler for installasjon og oppsett av EVA-applikasjonene.
- Lokaler for test av maskinvare og valgmateriell.

3.2.2 Lokaler for stemming under valggjennomføringen



Mottak av forhånds- og valgtingsstemmer skal foregå i grønn sone, registrering av stemmer i manntallet skal foregå i rød sone.

Av den grunn må man dele lokalet inn i to soner:

- En grønn sone for publikum med valgavlukker og ubrukte stemmesedler.
- En rød sone for maskinvare og manntall – tydelig adskilt fra publikum for å sikre valgets integritet og ivareta tilgangsbegrensning til maskinvaren og manntallet.

I praksis betyr dette at velgere aldri skal ha tilgang til PC-er eller avkrysningsmanntall der stemmer registreres.

3.2.3 Transport av stemmesedler mellom valglokale og opptelling

Transporten av stemmesedler fra stemming til opptelling er en kritisk del av valggjennomføringen og har følgende krav:

- Kjøretøyet som benyttes er å anse som rød sone fra transport starter til den avsluttes. Dersom det benyttes kollektiv eller kommersielle transportører er det kommunen eller fylkeskommunens ansvar å sikre at transportør oppfyller kravene til rød sone ved transport.
- Transporten skal skje i forseglede beholdere og på en slik måte at transporten er rask og sikker.
- Forsegling av beholdere skal gjøres før overlevering til transportør, og transportør skal ikke ha tilgang til forseglingsutstyr.
- Overlevering ved transportstart og -slutt skal alltid være bemannet og overlevering skal dokumenteres og kontrolleres av mottaker.

- Ved overlevering til transportør skal det kvitteres ut:
    - Hvem som avleverer.
    - Hvem som er transportør.
    - Hva som overleveres.
    - Hvor mange kolli, og hvilke kollier som overleveres.
    - Tid for overlevering.
    - Sted for overlevering.
- Ved transportørs overlevering til opptellingssted skal det kvitteres ut:
    - Hvem som avleverer.
    - Hvem som er mottaker.
    - Hva som overleveres.
    - Hvor mange kolli, og hvilke kollier som overleveres.
    - Tid for overlevering.
    - Sted for overlevering.

3.2.4 Lokaler for opptelling under valggjennomføringen

Opptelling av stemmesedler skal være offentlig. Samtidig er det viktig at tilgang til maskinvare og valgmateriell begrenses for å minimere mulighetene for sabotasje eller andre uønskede tilsiktede eller utilsiktede hendelser.

Av den grunn må man dele inn i to soner:

- En grønn sone hvor publikum kan observere opptellingen – for å sikre allmenn tilgjengelighet og ivareta tillit til valggjennomføringen.
- En rød sone for maskinvare og valgmateriell – tydelig adskilt fra publikum for å sikre valgopptellingens integritet og ivareta tilgangsbegrensning til materiell og maskinvare.

Publikum og besøkende som ønsker å overvære opptellingen skal oppholde seg i grønn sone. Den røde sonen skal være et avgrenset område innenfor den grønne.

Maskinvare og valgmateriell som benyttes til opptellingen skal plasseres og oppbevares trygt innenfor rød sone. Kun autorisert personell skal ha tilgang til sonen. Sonen kan for eksempel avgrenses med sperrebånd. Vakthold besørges av eget personell eller av medarbeidere med tilgang til rød sone. Det er viktig at vakten har kontroll på at ingen uten akkreditering passerer avgrensningen mellom grønn og rød sone.

4 Organisasjon og mennesker

I NSM sine veiledere er organisatoriske og menneskelige sikkerhetstiltak to forskjellige kapitler. Vi har valgt å slå disse sammen for å samle *minimumsnivået* av tiltakene under ett kapittel.

Hensikten med disse sikkerhetstiltakene er å sette opp menneskelige og organisatoriske barrierer mot uønskede og tilsiktede handlinger.

Barrierene er tiltak i form av skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, adferd og/eller anvendelser av sikkerhetstiltak. Sikkerhetstiltakene kan blant annet etableres i form av skilting, opplæring og bruk av adgangskort.

4.1 Kompetanse

Valgmedarbeidere bør læres opp i sikkerhet. Alle valglokaler har en leder og nestleder som har økt ansvar for stemmingen i det enkelte lokale. Det er derfor viktig at leder og nestleder har god kjennskap til sikkerhet i valggjennomføringen. Opplæringen bør i hovedsak bygge på denne veilederen og kommunens planverk (se 4.1.3).

4.2 Personellsikkerhet

Personer som jobber med valggjennomføringen blir vist høy tillit – både av kommunen og fylkeskommunen, men også av samfunnet for øvrig.

Valgmedarbeidere har tilgang til valgsystemene og andre kritiske aspekter ved valget. Valgmedarbeidere kan, med eller uten hensikt, utføre handlinger som ikke er ønskelige. Det er derfor viktig at valgmedarbeiderne, så langt det er mulig, er personer som er til å stole på. Det er også viktig at personellet er klar over at de ufrivillig kan bli utsatt for påvirkning som en del av en større sikkerhetshendelse, uten at de vet om det, samt at de kan bli truet til å gjøre en handling.

Det er ikke nødvendig med sikkerhetsklarering på personell som jobber med valget, med mindre personellet skal ha tilgang til gradert informasjon som for eksempel trusselvurderinger og sårbarhetsrapporter. Valgdirektoratet anbefaler likevel sterkt at valgstyret påser at alle som jobber med valggjennomføringen får en sikkerhetsorientering om trusler, sikkerhetstiltak og rutiner som enten direkte eller indirekte kan påvirke deres mulighet til å utføre jobben de settes til å gjøre.

4.3 Planverk

Kommunene og fylkeskommunenes planverk bør inneholde relevante rutiner knyttet til sikkerhet. Disse bør inneholde regler for hvordan valgmedarbeidere skal gjøre jobben sin sikkert og hvordan andre organisatoriske tiltak skal utføres. Viktigst av disse er:

- Rutine for sikkert mottak av stemmesedler.

- Rutine for transport av stemmesedler fra valglokale til opptellingslokale.
- Regler for bruk av IKT utstyret.
- Varslingsrutine for hendelser.
- Tydelige kommunikasjonslinjer ved sikkerhetshendelser.
- Sikkerhetsledelse.
- Skilting.
- Avlåsingsregime.

Kommunene og fylkeskommunene bør også etablere et planverk for hendelseshåndtering som ivaretar valggjennomføringen ved beredskap og krise. Planverket bør inkludere en oversikt over:

- krav til gjenopprettelse av IKT- funksjoner, IKT-tjenester og IKT-systemer - basert på en analyse av konsekvenser for valggjennomføringen,
- rolle- og ansvarsbeskrivelser for relevant personell,
- krav til opplæring for relevant personell,
- klassifiseringsregime for hendelser og grenseverdier for å aktivere krisestab,
- krav til testing og øving av planverk og personell.

Det er viktig å revidere og oppdatere planverket jevnlig, som minst én gang hvert valg og i etterkant av øvelser og større hendelser eller angrep. Små og store øvelser bør gjennomføres regelmessig.

4.4 Sikker tjenesteutsetting

Kommunene og fylkeskommunene er ansvarlig for sikkerheten ved tjenesteutsetting av IKT-leveranser.

Dette inkluderer å ha oversikt og kontroll på hele livsløpet til tjenesten(e) som skal settes ut, ivareta behovet for bestiller-kompetanse (f.eks. forvaltning-, administrasjon- og IT- arkitekturkompetanse) gjennom hele livsløpet til tjenesteutsettingen, gjennomføre gode risikovurderinger som inkluderer hele livsløpet, utarbeide et kravdokument for alle faser av tjenesteutsettingen hvor krav kan verifiseres, avtaler om tjenesteutsetting av IKT-tjenester. Det er viktig med god kontroll på leverandørene og de tilhørende verdikjedene til leveransene.

5 Informasjonssikkerhet ved bruk av EVA

Valgdirektoratet har en rekke tiltak som vi anbefaler at kommuner og fylkeskommuner innfører når EVA-applikasjonene tas i bruk. Anbefalingene i dette kapittelet omhandler bruk av alle EVA-applikasjonene og gjelder i alle faser av valggjennomføringen.

Tiltakene bør tilpasses behovet til de ulike rollene i valggjennomføringen. For eksempel har en person med rollen *valgansvarlig* ofte behov for mer funksjonalitet, flere programmer og fysiske tilganger, enn en person som kun skal ta imot stemmer i et valglokale.

For de som benytter EVA Skanning er det ytterligere noen anbefalinger beskrevet i neste kapittel.

Det følger lovkrav til enkelte tiltak. Slike tiltak må implementeres for å oppfylle kravene til informasjonssikkerhet gitt i valgforskriften. Hjemmelen for det enkelte tiltak er synliggjort i egen boks under hvert tiltak. Selv om kun noen av tiltakene er påkrevd, understreker vi at Valgdirektoratet anbefaler at kommunene og fylkeskommunene implementerer samtlige tiltak som beskrives under.

Anbefalingene gjelder også for tredjeparter som bistår kommuner og fylkeskommuner med teknisk støtte. Ofte vil en slik avtale dekke deler av rollen IKT-ansvarlig vanligvis har. Dette må avklares mellom den enkelte kommune eller fylkeskommune og leverandør av teknisk bistand.

De fleste kommuner benytter seg av Windows ved gjennomføringen av valget. Vi tar derfor dette som utgangspunkt i de tekniske anbefalingene. Benytter kommunen et annet operativsystem slik som iOS/Android på nettbrett, eller Linux/MacOS på PC må kommunen sette seg inn i innskrenkningsmekanismene som gjelder for deres operativsystem. Uavhengig av valg av operativsystem bør *prinsippene* i dette kapittelet følges.

5.1 PC-er

PC-ene som brukes til EVA bør være nye, eller være i et kontrollregime som ivaretar kravene til sikkerhet. Sikring iht. punkt 3.2 i veilederen, der maskinene sikres slik gjennom hele sitt livsløp, anbefales sterkt.

Anbefalinger om at PC-ene er nye eller har vært sikret tidligere, gis for å sikre kommunene mot at uvedkommende får uautorisert tilgang til EVA, eller på andre måter angriper maskinene.

Anbefalingene minimerer også risikoen for at valggjennomføringen i kommunen hindres, eller at det sås tvil om at valgresultatet i kommunen er riktig.

Anbefalingene knyttet til PC-er gis også for å skape større grad av sikkerhet rundt opphav og oppbevaring av PC-ene som brukes i valggjennomføringen.

5.2 Windows 11 Enterprise

Windows-PCer hvor EVA benyttes bør kjøre operativsystemet Windows 11 Enterprise. Ved valg av andre versjoner av Windows kan det være utfordringer knyttet til å ta i bruk innskrenkningsmekanismer. Dersom kommunen tar i bruk andre operativsystemer enn Windows, må kommunen selv verifisere at innskrenkningsmekanismene kan implementeres.

Anbefalingen om bruk av Windows 11 Enterprise gis for å begrense internett- og applikasjonstilgang fra PC-ene ved hjelp av innskrenkningsmekanismer som kun finnes i denne versjonen av Windows. Ved hjelp av disse mekanismene vil det kun være mulig å bruke applikasjoner og internett-tjenester som er nødvendige for å bruke EVA. Alle andre tilganger og applikasjoner kan blokkeres.
Ved å begrense applikasjons- og internettilgangen på PC-er der EVA brukes, begrenses også angrepsflaten og mulighetene for kompromittering.

5.3 Kontrollert fjerntilgang

Fjerntilgang for leverandører av teknisk støtte til kommunene må skje i kontrollerte former og under overvåking av autorisert personell hos kommunen/fylkeskommunen. Fjerntilgang gir muligheten til å koble seg opp på maskinen uten fysisk tilgang til den, og denne muligheten benyttes ofte i forbindelse med feilsøking og brukerstøtte.

Vedvarende fjerntilgang må derfor deaktiveres på maskiner som skal benyttes til EVA. Skulle det være nødvendig med fjerntilgang for å utføre støtte, skal denne initieres av autorisert personell fra EVA maskinen i det den skal benyttes.

Det er den enkelte kommune eller fylkeskommune som bestemmer om man vil benytte seg av fjerntilgang, og når dette skal skje. I så fall må kommunen eller fylkeskommunen åpne for dette i henhold til en avtalt prosedyre med utveksling av nødvendige koder for å kunne logge seg inn.

> Kommunen eller fylkeskommunen skal sørge for forsvarlig tilgangsstyring på maskinene som benyttes for å få tilgang til det elektroniske valggjennomføringssystemet, jf. valgforskriften § 4-2 (1).

5.4 Sertifikater

Klientsertifikatene utstedes av Valgdirektoratet for å øke nettverkssikkerheten for pålogging i EVA. Distribusjon av klientsertifikatet må foregå på en sikker og trygg måte. Sikkerheten økes ved å sikre at det kun er godkjente klienter i organisasjonen

som kan brukes til å logge seg inn. Sertifikatene er unike for hver kommune og fylkeskommune, og kontrolleres og logges av Valgdirektoratet.

Dersom et sertifikat kommer på avveie, skal det meldes til Valgdirektoratet umiddelbart. Valgdirektoratet vil da gjøre sertifikatet på avveie ugyldig og utstede et nytt.

5.5 Maskiner skal låses når de forlates

5.5.1 Rød sone

Operativsystemet skal låses når maskinen forlates slik at uvedkommende ikke får tilgang til det den innloggede brukeren har tilgang til.

5.5.2 Grønn sone

Forlates maskinen i en grønn sone skal maskinen også låses ned i skuff, skap eller lignende, eventuelt kan maskinen legges i en forseglingspose. Se punkt 3.2. om fysisk sikring.

Kommunen eller fylkeskommunen skal sørge for forsvarlig tilgangsstyring på maskinene som benyttes for å få tilgang til det elektroniske valggjennomføringssystemet, jf. valgforskriften § 4-2 (1).

5.6 Tilgangsstyring

Alle som jobber i EVA-applikasjonene, får tildelt personlige brukere i EVA og det er derfor aldri behov for å låne bort sin personlige bruker. Lånes brukeren bort kan det føre til at du selv blir ansvarlig for feil andre måtte gjøre.

Tilgangsstyring på maskiner kan gjennomføres på ulike måter. For eksempel kan det gjøres ved å sørge for at enhver person som skal bruke maskiner med tilgang til det elektroniske valggjennomføringssystemet har en personlig brukertilgang, eller ved at det føres oversikt over hvem som benytter en maskin.

Dersom kommunen eller fylkeskommunen velger å føre oversikt over hvem som benytter de ulike maskinene, bør det også etableres rutiner som sørger for hvem som fører denne oversikten. Oversikten bør inneholde *hvem*, *hvilken maskin*, og *tidspunkt (ev. tidsintervall)*.

Kommunen eller fylkeskommunen skal sørge for forsvarlig tilgangsstyring på maskinene som benyttes for å få tilgang til det elektroniske valggjennomføringssystemet, jf. valgforskriften § 4-2 (1).

Kravet i forskriften omhandler at kommunen eller fylkeskommunen skal sørge for tilgangsstyring på de aktuelle maskinene. Anbefalingene og bør-omtalen rundt rutiner fremgår ikke av regelverket, men er sterkt anbefalt.

5.7 Passord

Alle standardpassord på all maskinvare bør endres før produksjonssetting. Dette inkluderer applikasjoner, operativsystemer, rutere, brannmurer, skrivere og skannere m.m. I den grad maskinvaren støtter det, bør man benytte sertifikatbasert autentisering og redusere mulighet for passordbasert autentisering over nettverket. MFA (multifaktorautentisering) bør være hovedregel for all brukerautentisering.

5.8 Oppgrader program- og maskinvare og installer sikkerhetsoppdateringer

Selv de beste datamaskiner, enheter og applikasjoner kan ha feil og sårbarheter som kan utnyttes av angripere. Valgdirektoratet anbefaler derfor at kommunene og fylkeskommunene sørger for å kun benytte produktversjoner som fortsatt støttes og mottar sikkerhetsoppdateringer fra leverandøren. Eldre IKT-produkter må da fases ut, og oppdateringer må installeres.

Nyere produktversjoner inneholder funksjonelle og sikkerhetsrelaterte forbedringer, og de har ofte flere og bedre sikkerhetsfunksjoner. Kommunene og fylkeskommunene bør etablere et sentralt styrt regime for oppdatering av applikasjoner, operativsystemer og fastvare, slik at sluttbrukere ikke kan velge bort å installere nødvendige oppdateringer.

Husk også å be tjeneste-leverandører informere om risikoer og sårbarheter produktet kan utsettes for, og spesifisere nærmere hvordan IKT-produktet kan sikkerhets-herdes og beskyttes.

5.9 Ikke tildel administratorrettigheter til sluttbrukere

De fleste valgmedarbeidere har ikke behov for administratorrettigheter. I et sentralt administrert system kan valgmedarbeidere få den programvaren de trenger fra et felles distribusjonspunkt. Det er heller ikke behov for administratorrettigheter for å kunne bruke EVA-applikasjonene.

Dette gjelder også fordeling av roller i EVA. Ikke gi valgmedarbeidere roller i systemet som de ikke trenger for å utføre oppgaven sin. Dette reduserer muligheten for innsidevirksomhet og kan redusere skadeomfanget dersom en brukerpålogging kommer på avveie.

Kommunen eller fylkeskommunen skal sørge for forsvarlig tilgangsstyring og å begrense funksjonalitet på maskinene som benyttes for å få tilgang til det elektroniske valggjennomføringssystemet, jf. valgforskriften § 4-2 (1).

Dette kapittelet gir anbefalinger for hvordan personer som får tilgang til maskiner ikke skal få tilgang til funksjonalitet utover det som ligger til arbeidsoppgavene de skal utføre.

5.10 Blokker kjøring av ikke-autoriserte programmer («hvitelisting»)

Bruk verktøy som «Windows AppLocker» for å kontrollere at sluttbrukere kun får kjøre godkjente applikasjoner og de applikasjoner som de har bruk for i valggjennomføringen.

Ved installasjon av EVA Skanning blir en AppLocker policy også satt opp på maskinen. Til EVA Admin anbefales det å bruke AppLocker konfigurasjonen som ligger tilgjengelig i vedlegg 3.

AppLocker policyen oppdateres ved behov, oppdateringer blir varslet via Valgdirektoratets nyhetsbrev.

Kommunen eller fylkeskommunen skal sørge for å begrense funksjonalitet på maskinene som benyttes for å få tilgang til det elektroniske valggjennomføringssystemet, jf. valgforskriften § 4-2 (1).

Dette kapittelet gir anbefalinger for hvordan personer som får tilgang til maskiner ikke skal få tilgang til funksjonalitet utover det som ligger til arbeidsoppgavene de skal utføre.

5.11 Deaktiver enheter og funksjonalitet som ikke brukes

Deaktiver enheter og funksjonalitet som ikke brukes under valget. Bluetooth skal deaktiveres, og trådløst internett bør deaktiveres dersom kablet nettverk administrert av kommunen er tilgjengelig. Enheter som kamera, infrarød, pcmcia, firewire og com/lpt porter bør også deaktiveres. Den sikreste måten å deaktivere dette på er i maskinens fastvare, eksempelvis BIOS. Se leverandørens dokumentasjon på hvordan dette gjøres.

Kommunen eller fylkeskommunen skal sørge for å begrense funksjonalitet på maskinene som benyttes for å få tilgang til det elektroniske valggjennomføringssystemet, jf. valgforskriften § 4-2 (1).

Dette kapittelet gir anbefalinger for hvordan personer som får tilgang til maskiner ikke skal få tilgang til funksjonalitet utover det som ligger til arbeidsoppgavene de skal utføre. I tillegg vil de anbefalte tiltakene redusere angrepsflaten og risikobildet.

5.12 Herde applikasjoner

Protected Mode/View for nettleseren, Microsoft Office og Adobe Reader begrenser skadeomfanget ved kompromittering. Deaktiver unødvendig mobil kode og makroer. For å herde f.eks. Windows og Microsoft Office kan Microsoft Security Compliance Toolkit[1] benyttes.

Enhver ny applikasjon og funksjon øker mulighetene for angrep. Valgmedarbeidere har for eksempel ikke behov for Java Runtime eller JavaScript i Adobe Reader. Unødvendig programvare bør fjernes. Alle applikasjoner må herdes og holdes oppdatert, noe som øker administrasjonsbyrden på systemet.

> Kommunen eller fylkeskommunen skal sørge for å begrense funksjonalitet på maskinene som benyttes for å få tilgang til det elektroniske valggjennomføringssystemet, jf. valgforskriften § 4-2 (1).
>
> Dette kapittelet gir anbefalinger for hvordan personer som får tilgang til maskiner ikke skal få tilgang til funksjonalitet utover det som ligger til arbeidsoppgavene de skal utføre. I tillegg vil de anbefalte tiltakene redusere angrepsflaten og risikobildet.

5.13 Klientbrannmur

Nyere versjon av Windows brannmur støtter filtrering av utgående trafikk med dynamiske nøkler (FQDN). Merk at dette må konfigureres korrekt (se hvordan her) Windows Brannmur bør settes opp slik at den blokkerer all trafikk initiert utenfra og kun åpner for de domenene som skal benyttes og annen nødvendige trafikk, som DNS, WSUS og DHCP ut fra klienten.

Vi anbefaler bruk av nettleseren Chrome, Via GPO bør man så konfigurere Chrome til å kun tillate tilgang til en liste med domener/URL-er. Valgdirektoratet vedlikeholder en slik liste nødvendig for EVA i vedlegg 2.

[1] https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

Brannmuren bør også settes opp slik at den logger sikkerhetsrelevante hendelser. Disse loggene bør inspiseres regelmessig.

Kommunen eller fylkeskommunen skal sørge for å begrense datatrafikk og funksjonalitet på maskinene som benyttes for å få tilgang til det elektroniske valggjennomføringssystemet, jf. valgforskriften § 4-2 (1).

Dette kapittelet gir anbefalinger for hvordan klientbrannmuren kan settes opp for å begrense datatrafikken. Valgdirektoratet vedlikeholder en liste over de domenene som det minimum må åpnes for å bruke EVA. Dersom enkelte medarbeidere i kommunene eller fylkeskommunene har behov for at det åpnes for flere domener, så må det også åpnes for disse i brannmuren.

5.14 Nettverk

Nettverk som benyttes i forbindelse med valggjennomføringen, for eksempel i et valglokale bør være et nettverk som er kontrollert av kommunen/fylkeskommunen. Der det er mulig bør kablet nettverk benyttes. Dersom trådløst internett benyttes, anbefaler direktoratet sterkt at dette er passordbeskyttet og at tilgangen til nettverket er begrenset.

Mobilt trådløst bredbånd kan benyttes i de tilfeller der kommunen ikke har anledning til å sette opp eget sikret nettverk.

5.15 Sikker oppstart og diskkryptering

Aktiver Sikker oppstart (Secure Boot) og Windows BitLocker. Denne funksjonaliteten bruker maskinvare- og harddiskkryptering for å oppdage manipulering av oppstartsprosessen og forhindre tap av data fra stjålne/tapte PC-er.

5.16 Antivirus/antiskadevare

Antivirus oppdager og blokkerer kjent skadevare som bl.a. utnytter sårbarheter i epost-programmer og dokumentlesere. Fortrinnsvis bør man bruke et produkt som kan styres sentralt og som virker bra sammen med operativsystemet. På Windows 11 er Windows Defender slått på som standard, og det dekker denne anbefalingen.

5.17 Monitorering

Valgdirektoratets verktøy for monitorering av operativsystemet bør installeres. Verktøyet monitorerer aktivitet som utføres på klienten den er installert på og vil gjøre det mulig for Valgdirektoratet å bruke loggene ved en eventuell hendelseshåndtering.

Det er kun krav om å benytte programvaren for klientmonitorering på maskiner som benyttes til å telle stemmesedlene maskinelt, jf. valgforskriften § 4-2 (2).

Valgdirektoratet anbefaler imidlertid at programmet installeres på alle maskiner som skal brukes, slik at direktoratet får et oppdatert situasjonsbilde og kan i større grad varsle kommuner og fylkeskommuner ved hendelser.

5.18 Tilbakestilling

Etter at valggjennomføringen er over bør alle maskiner som har vært i bruk i forbindelse med valget tilbakestilles til fabrikkinnstillinger. Det vil si at harddisken på maskinen renses på betryggende måte og at operativsystem installeres på nytt før maskinen brukes til andre oppgaver. Unntaket gjelder maskiner som skal brukes til fremtidig valggjennomføring, som bør oppbevares iht. rød sone etter tilbakestilling.

Dette sikrer at sensitive valgdata ikke kommer på avveie. Som for eksempel påloggingsinformasjon, uttrekk fra manntallet, andre rapporter, m.m.

6 Ekstra tiltak ved bruk av EVA Skanning

For å telle stemmer maskinelt ved å benytte EVA Skanning har vi utarbeidet en liste med ekstra tiltak for denne maskinvaren. Det er viktig at alle tiltakene i kapittel 5 også er gjennomført. Denne listen er ytterligere tiltak spesielt rettet mot maskinell telling.

6.1 Installasjon av EVA Skanning

Installasjon og oppsett av EVA Skanning skal følge installasjonsveiledningen som distribueres med EVA Skanning. Installasjonsprosessen er utformet for å gi en mest mulig kontrollert og sikker installasjon av EVA Skanning.

6.2 Tilstandsrapportering og logging

Av sikkerhetshensyn ønsker Valgdirektoratet å kjenne tilstanden for PC-er der EVA Skanning er installert for maskinell telling av stemmesedler. PC-er der EVA Skanning er installert og som brukes til maskinell telling av stemmesedler vil derfor kontinuerlig rapportere sin tilstand og feilmeldinger til Valgdirektoratet.

Dette gjøres for å kunne avdekke avvik i oppsett og konfigurasjon som kan utgjøre en sikkerhetsrisiko, samt innhente statistikk om hvor mange PCer som er i bruk ved maskinell telling, for på den måten å forbedre tjenesten.

På disse maskinene er det derfor påkrevd at Valgdirektoratets løsning for endepunktsmonitorering installeres.

> Dersom kommunen eller fylkeskommunen skal benytte skanning for å telle stemmesedlene i andre telling, skal programvare for monitorering av operativsystemet benyttes, jf. valgforskriften § 4-2 (2).

6.3 Nettverk

Nettverket der EVA Skanning benyttes må sikres. Det fysiske nettverket (kabling, switcher, brannmurer, osv.) må sikres i henhold til rød sone.

Anbefalte tiltak:

- Sett opp et dedikert kablet nettverk til bruk for EVA Skanning.
    - Trådløst nettverk bør ikke benyttes
- Beskytt nettverket med perimetersikring mot omverden som kun tillater absolutt nødvendig trafikk ut (se vedlegg 2) og blokkerer all trafikk inn.

- Autoriser kun enheter som skal ha tilgang til nettverket.
- Trafikk mellom enheter krypteres.
- Sikre nettverket fysisk slik at man har kontroll på antall nettverkskontakter, kontaktenes plassering og tilkoblede enheter.
- Benytt portsikkerhet, eksempelvis IEEE 802.1X.

6.4 Perimetersikring

Perimetersikring i dette tilfellet handler om konfigurering av brannmur og/eller annen beskyttelse av det lokale nettverket der EVA Skanning er installert. For at EVA Skanning applikasjonen skal fungere må det legges inn åpninger i perimetersikringen. Dette kan for eksempel være brannmurer og andre mellomtjenere.

Valgdirektoratets IP adresser er 62.92.129.0/24 og vi anbefaler at det åpnes for alle protokoller mot vårt nettverk. Valgdirektoratet vedlikeholder også en liste med domener ut over våre egne IP-er i vedlegg 2.

Noen av domenene i listen vi vedlikeholder står bak CDN-nettverk hvor IP-adresser kan endre seg. Det anbefales derfor å benytte perimetersikring som kan basere seg på domenenavn istedenfor bare IP-port.

6.5 Antivirus

EVA Skanning er kun testet sammen med Windows Defender. Det anbefales derfor at Windows Defender er den eneste antivirus løsningen som benyttes på PCer som skal brukes til maskinell telling.

7 Vedlegg

- Vedlegg 1: Sjekkliste
- Vedlegg 2: Lister med domener og URL-er
- Vedlegg 3: AppLocker konfigurasjonsfil
- Vedlegg 4: Enkel ROS-mal med forklaringer

8 Referanseliste

- Digitaliseringsdirektoratet – Om risiko og risikovurdering: https://www.digdir.no/informasjonssikkerhet/om-risiko-og-risikovurdering/3048
- Direktoratet for samfunnssikkerhet og beredskap – Risiko, sårbarhet og beredskap: https://www.dsb.no/ros-og-beredskap/
- Nasjonal sikkerhetsmyndighet – Grunnprinsipper for IKT-sikkerhet: https://nsm.no/regelverk-og-hjelp/grunnprinsipper/grunnprinsipper-for-ikt-sikkerhet
- Nasjonal sikkerhetsmyndighet: https://nsm.no/
- Nasjonalt Etterretnings- og Sikkerhetssenter – ugradert trussel- og sårbahretsvurdering om stortings- og sametingsvalget 2025: https://valgmedarbeiderportalen.valg.no/media/y4rk43ht/ness-rapporten.pdf
- Valgforskriften § 4-2. Informasjonssikkerhet ved bruk av det elektroniske valggjennomføringssystemet: https://lovdata.no/forskrift/2024-11-05-2662/§4-2
- Veileder i sikkerhet med vedlegg: https://valgmedarbeiderportalen.valg.no/veiledere-og-rutiner/veiledere/sikkerhetsveileder/