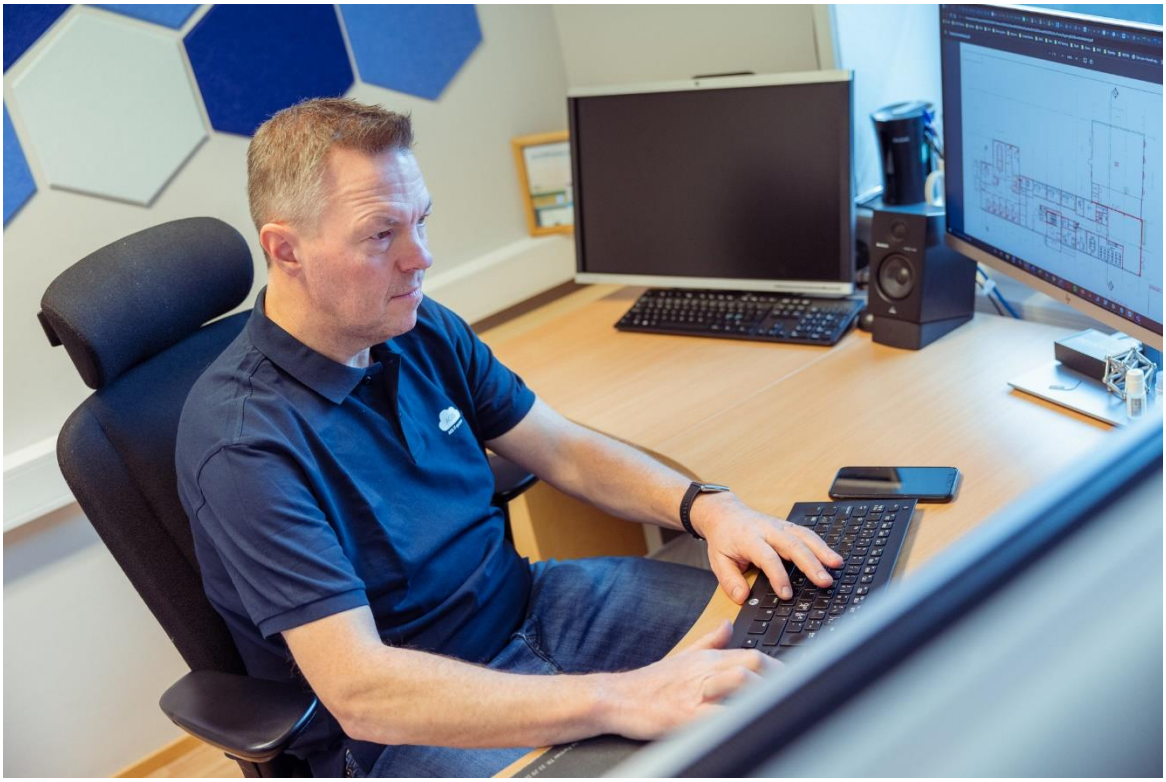
Sikkerhetspakke II - Microsoft 365 Intune MDM

Microsoft 365 MDM levert av AGS IT-partner

MDM (Mobile Device Management) er en komplett løsning for sikkerhets-administrasjon av PC og mobile enheter, som smarttelefoner, nettbrett og bærbare datamaskiner.



Hva gjør Microsoft 365 Intune for deg

Microsoft Intune er en skytjeneste som administrerer klienter som PC, Mac, mobil og nettbrett. Med Intune bestemmer du hva slags standard sikkerhets-policy alle enhetene i bedriften skal ha.

- Du definerer hvilke data og applikasjoner brukerne kan få tilgang til, samt hva de kan gjøre med dataene. Microsoft 365 Intune er inkludert i Microsoft 365 Business Premium.

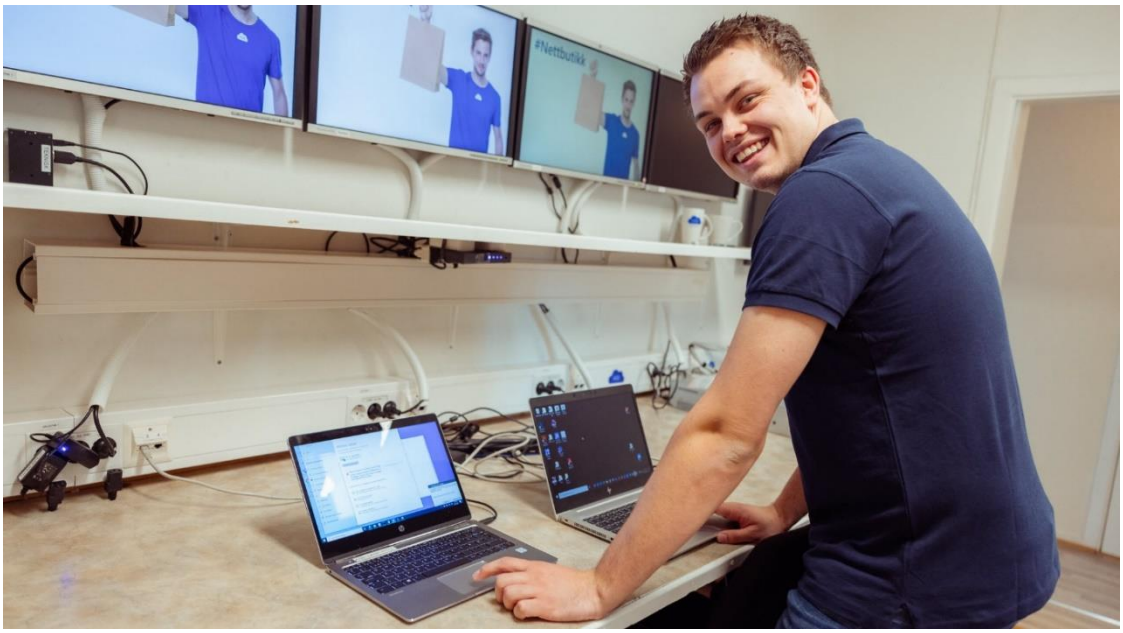
Intune er en komplett sikkerhetstjeneste og MDM løsning fra Microsoft. Intune hjelper deg til å automatisk sette, administrere, overholde sikkerhetsstandarden i bedriften for alle brukere og enheter.

- Intune kan automatisk rulle ut de riktige applikasjonene som brukeren trenger.
- Løsning lar deg administrere og få kontroll over alle maskiner og mobile enheter i bedriften.
- Systemet setter en felles sikkerhets-policy som enhetene må oppfylle.
- Du får sikkerhetskopi av lokale filer på maskinen din til OneDrive for Business.
- Etterfølger Microsoft beste standard for sikkerhet.
- Autopilot for automatisk utrulling av applikasjoner på nye maskiner
- Fjernslette enheter som blir stålet, mistet eller som blir «offboardet» når en ansatt slutter.
- Hjelpe deg med å separere bedriftsdata fra private data på enhetene til brukerne.

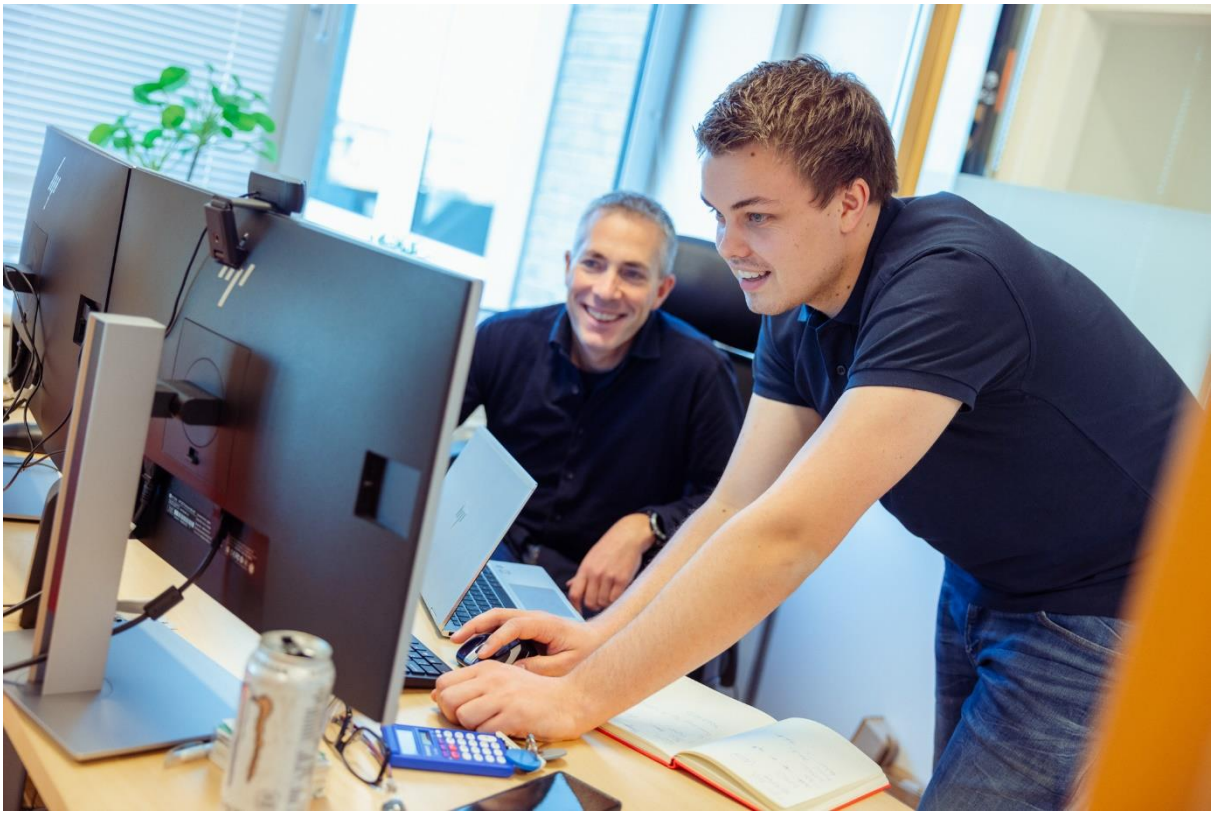
⭕ **Eksempel:** En maskin eller enhet blir mistet/stjålet fra en ansatt. Her kan du med noen enkle tastetrykk fjerne all arbeidsrelatertdata fra maskinen/enheten.

Slik setter vi opp Sikkerhetspakke II MDM for deg

Følgende utføres av tekniker fra AGS IT-partner, og er inkludert i oppsettet og etablering av MDM.



Microsoft 365 Business Premium	Sikkerhets pakke I MFA	Sikkerhets pakke II MDM
2-faktor-autentisering (MFA)	●	●
Defender for Office sikrer e-post mot spam, farlige lenker og vedlegg	●	●
Enkel og selvbetjent tilbakestilling av passord (self-service password-portal)	●	●
Company branding for å enklere avsløre svindelforsøk	●	●
E-post kryptering	●	●
BitLocker – kryptering av PC ved tyveri eller når enheten mistes	●	●
MDM (Intune) - sikring av alle enheter (PC, Mac, mobil og nettbrett	○	●
Fjernsletting av enheter og data dersom enhet blir stjålet eller bruker endrer arbeidsplass.	○	●
Automatisk øke sikkerhetsinnstillinger på enheter og programvare. (krav til passord lengde og kompleksitet)	○	●
Sikkerhetspolicy for bedriften (best practise fra Microsoft og AGS IT-partner)	○	●
Sørger for at sikkerhetsoppdatering på enheten er installert slik at maskinen ikke er en sikkerhetsrisiko i bedriften	○	●
Autopilot – tjeneste for automatisk utrulling av PC og programvare	○	●
Opprette en dedikert e-post adresse for Apple-id og Google play.	○	●
Enhet er i overenstemmelse i forhold til standard om antivirus, brannmur og kryptering (BitLocker)	○	●
Automatisk nedlastning av følgende applikasjoner på PC *(Teams, Outlook, OneNote, Excel, Access, PowerPoint, Publisher, Word)*	○	●
Sikkerhetskopi aktivering for dokumenter lagret i OneDrive mappen på PC-en *(Skrivebord, dokumenter og bilder)*	○	●
Inkluderer 1 time Workshop	○	●
Etablering, befaring og oppsett bedrift	**8.900,-**	**9.900,-**
Oppsett pr. ansatt *__Sikkerhetspakke II__ (__MDM)__ forutsetter at __Sikkerhetspakke I (MFA)__ er satt opp.	+ 250,-	+ 1990,-



Dette vil vi aktivere for deg i Sikkerhetspakke II MDM

Sikkerhetspolicy Windows:

- Aktivere BitLocker. (kryptering av data på maskinen)
- Aktivere sikker oppstart av PC (secure boot)
- Alltid siste Quality & Future updates til Windows. (Windows 10 eller 11 Pro)
- Alltid siste oppdaterte Office pakke med programvare.
- Utrulling av Microsoft programvare og apper i Microsoft 365
- Kontroll av at siste aktive sikkerhets oppdateringer er installert på enheten.
- Produktive oppdateringer på Office pakken (ta vekk unødvendig støy, sette regler for Outlook kalender).
- Aktivere brannmur som standard
- Kontrollere at antivirus og brannmur er aktivt og installert på maskinen.
- Aktivere Autopilot for utrulling av ny PC

Sikkerhetspolicy Mac:

- Beskyttelse av filstrukturen som er definert av Apple slik at skadelig programvare ikke kan få tilgang.
- Kontroll at siste aktive sikkerhets oppdateringer er installert på enheten.
- Kontrollere at maskinen er passord beskyttet med minimum 8 karakterer.
- Sette maskinen i låsemodus etter 15 minutter ved inaktivitet.
- Aktivere kryptering av maskinen.
- Utrulling av Microsoft programvare og apper i Microsoft 365
- Aktivere brannmur.

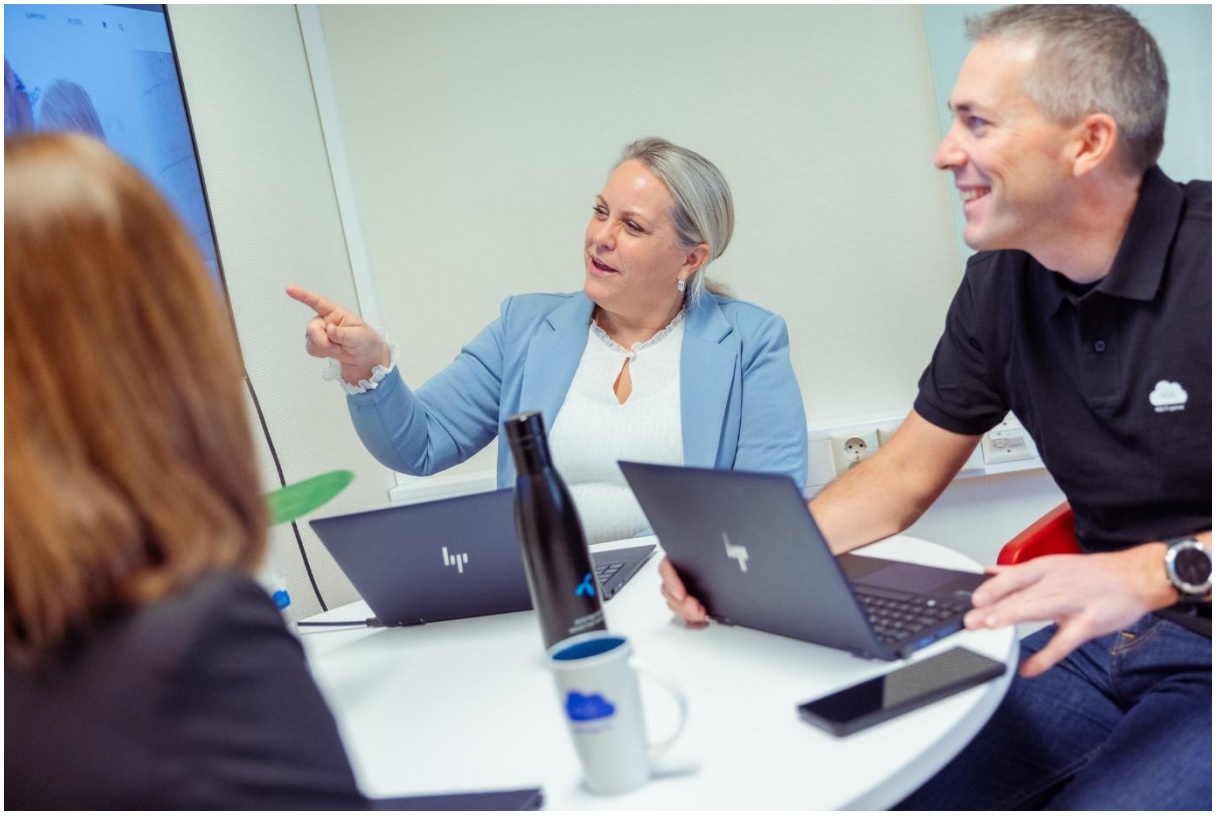
Sikkerhetspolicy iPhone/iPad:

- Jailbreak enheter blir blokkert fra firma ressurser.
- Kontroll at siste aktive sikkerhets oppdateringer er installert på enheten.
- Kontrollere at alle aktive mobiler har låsekode aktivert.
- Kontrollere at alle aktive mobiler har 6-siffer i låsekoden.
- Sette låsekode til å skru seg på med en gang mobilen går i «dvale».
- Sette innstilling at mobilen skal gå i dvale av seg selv etter 5 minutter.
- Sørge for at følgende apper er installert: Outlook, Authenticator og Firmaportal (Intune for mobil).

Sikkerhetspolicy Android:

- Jailbreak enheter blir blokkert fra firma ressurser.
- Kontroll at siste aktive sikkerhets oppdateringer er installert på enheten.
- Kontrollere at alle aktive mobiler har låsekode aktivert.
- Kontrollere at alle aktive mobiler har 6-siffer i låsekoden.
- Blokkere apper fra ukjente kilder (ikke google play).
- Blokkere muligheten for å hacke mobil ved bruk av USB.
- Sette låsekode til å skru seg på med en gang mobilen går i «dvale».
- Sette innstilling at mobilen skal gå i dvale av seg selv etter 5 minutter.
- Sørge for at følgende apper er installert: Outlook, Authenticator og Firmaportal (Intune for mobil).
- Kryptere data på enheten.

⭕ **TIPS!** Mulighetene her er mange og bestemmes av hva organisasjonen din ønsker som regelsett. Når alle enheter og brukere er innrullet i Intune løsningen, vil gjennomføring av sikkerhetspolicy og vedlikehold gjøres enkelt med noen få tastetrykk.



Innledende Workshop

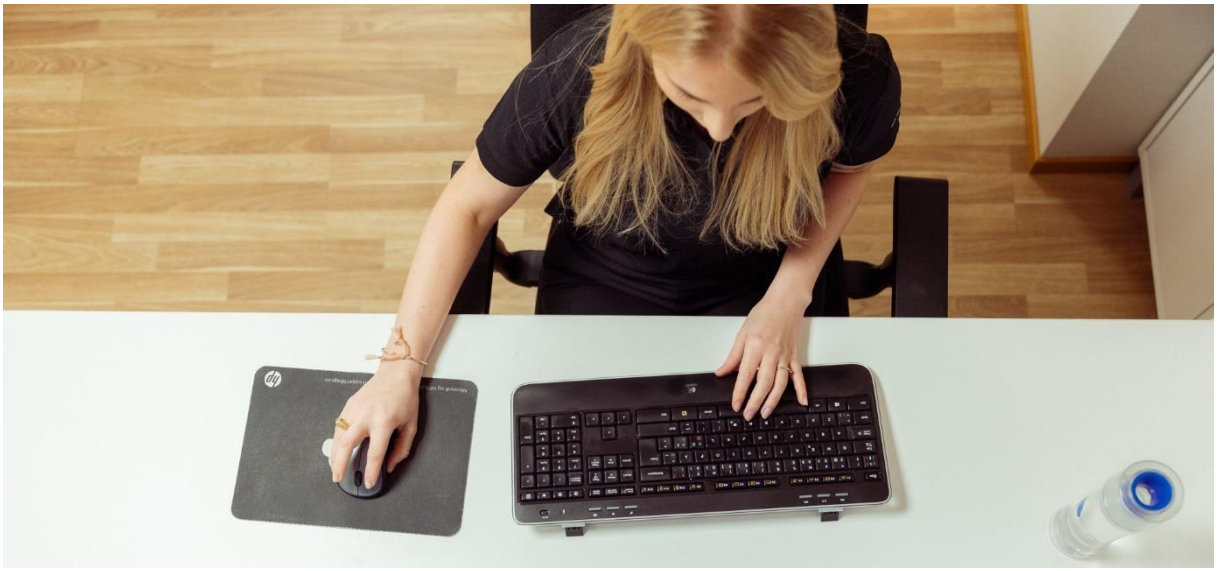
- Du får inkludert 1 time til en innledende Workshop der du får hjelp av oss til å sette en sikkerhets-standard for bedriften. I workshopen gjennomgår vi sammen alle valgene med deg slik at du blir fornøyd med oppsettet.

Utvidet Workshop og pilot

- Ønskes egendefinert sikkerhetspolicy i forhold til standard anbefaler vi en utvidet Workshop (+2-4 timer)
- For bedrifter med egen intern server anbefaler vi en utvidet Workshop (+2-4 timer)

Pilot

- For mer enn 20 brukere anbefales en pilot fase med utvalgte bruker(e) for best resultat.



Noen forutsetninger for et vellykket oppsett

- ✓ På PC bør du kjøre **Windows 11 Pro** eller siste oppdaterte versjonen av **Windows 10 Pro**.
- ✓ Mac maskiner bør ha den nyeste eller nest nyeste utgaven av MacOS.
- ✓ På den mobile enheten bør helst de nyeste versjonene av **Android** eller **iOS** være installert.
- ✓ Maskinene/telefonene bør helst ikke være over 3 år gammel.
- ✓ **Du trenger Microsoft 365 Business Premium lisens,** Microsoft 365 Enterprise E3 lisens eller Microsoft 365 Enterprise E5 lisens.
- ✓ **Sikkerhetspakke I (MFA)** bør være satt opp før du går i gang med **Sikkerhetspakke II (MDM)**
- ✓ Dedikert Microsoft 365 konto\delt postboks for Apple-id og Google play.
- ✓ Trenger du hjelp til å få noen av de overnevnte punktene på plass, hjelper vi gjerne med dette, og fakturerer for medgått tid.

⭕ **TIPS!** Eldre maskiner over 3 år yter ofte dårligere enn sine nye "kollegaer". Slike maskiner leverer ikke en god nok brukeropplevelse, og kan fort ødelegge "gleden" for brukeren med den nye løsningen.

Dette trenger vi for et vellykket brukeroppsett

Når vi er klare for å flytte alle maskiner og telefoner over til Intune er det viktig at alle ansatte har tilgang til følgende:

- ✓ Passordet til jobb e-post
- ✓ Brukeren har en 6-sifret låsekode på mobilen sin
- ✓ Android enhet: Google Play konto og passord til denne
- ✓ Apple enhet; Apple-ID konto og passord til denne
- ✓ Oppdatert PC, Mac, mobil og nettbrett
- ✓ Brukeren har tatt back-up av filene sine til OneDrive
- ✓ Trenger brukeren hjelp til å få dette på plass, hjelper vi gjerne med dette, og fakturerer for medgått tid.

TA KONTAKT
start@ags.no