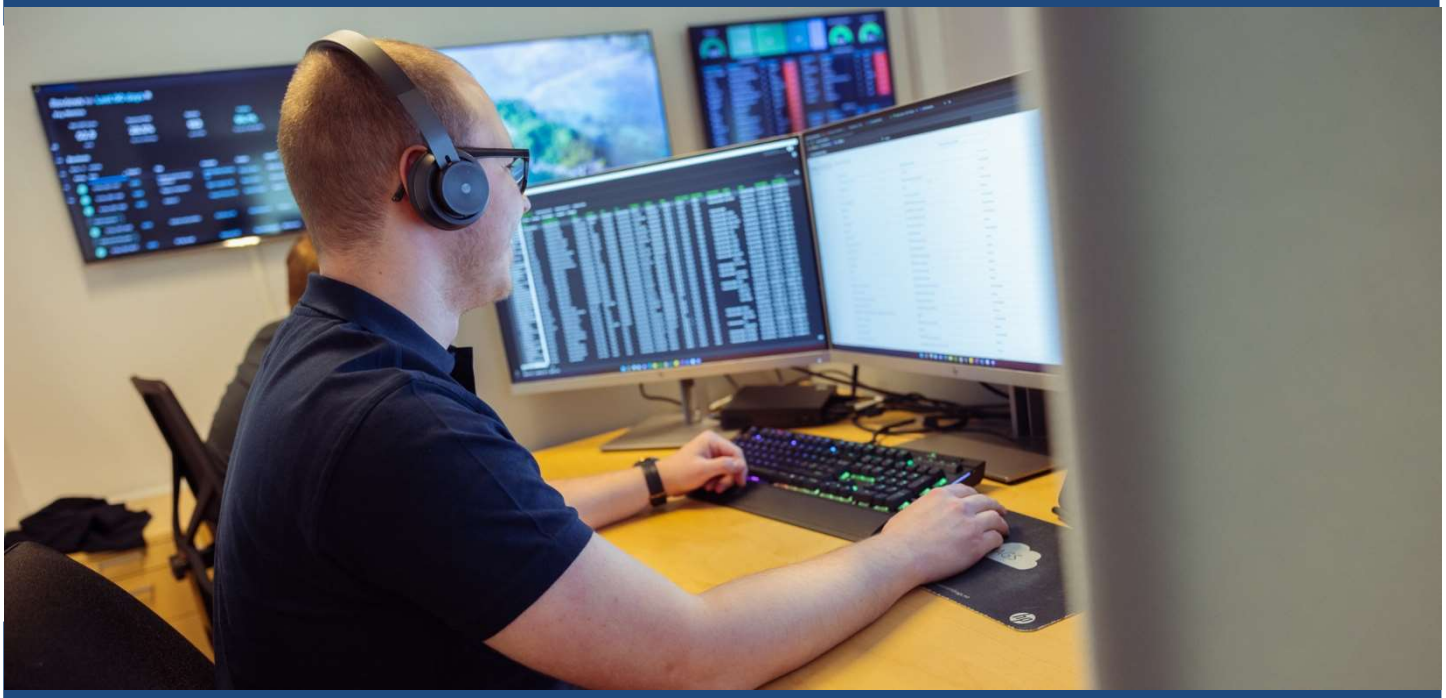

sikkerhetspolicy for PC, Mac og mobile enheter

Utarbeidet av **AGS IT-partner AS**

Versjon 2.1

Vedlegg 2: Anbefalt sikkerhetspolicy for PC, Mac og mobile enheter

1. Sikkerhetspolicy for PC-enheter

Nr.	Sikkerhetspolicy	Informasjon
1	**Aktivt antivirusprogram**	Oppdage, blokkere og fjerne skadelig programvare for å beskytte enheten mot skadelig programvare.
2	**Aktivert brannmur som standard**	Begrense uautorisert nettverkstilgang og beskytte enheten mot potensielle trusler utenfra.
3	**Microsoft BitLocker-kryptering er aktivert**	Beskytte sensitiv bedriftsinformasjon ved å kryptere data på maskinen og forhindre uautorisert tilgang ved tap eller tyveri.
4	**Aktivering av sikker oppstart**	Redusere risikoen for skadelig programvare ved å sikre at kun signert og pålitelig programvare kjører under oppstart.
5	**Alltid siste Quality & Future updates til Windows (Windows 10 eller 11 Pro)**	Sikre at operativsystemet er oppdatert med de nyeste kvalitets- og fremtidige oppdateringene for å opprettholde en høy sikkerhetsstandard.
6	**Automatiske sikkerhetsoppdateringer for Windows**	Opprettholde en høy sikkerhetsstandard ved å installere kontinuerlige oppdateringer og redusere sårbarheter.
7	**Siste oppdaterte Office-pakke**	Sikre at bedriftens produktivitetsprogramvare er beskyttet mot sårbarheter og utnyttelser.
8	**Kontroll av siste aktive sikkerhetsoppdateringer**	Bekrefte at alle nødvendige sikkerhetsoppdateringer er installert for å redusere risikoen for utnyttelse av kjente sårbarheter.
9	**Automatisk aktivering av låseskjerm etter 5 minutter**	Forhindre uautorisert tilgang når maskinen ikke er i bruk.
10	**Sikker passordpolicy**	Øke sikkerheten ved å implementere sterke passordpraksiser. -Store og små bokstaver. -Siffer -Minst ett spesialtegn -Minimum 8 karakterer Hvis pinkode benyttes, må denne være minimum 6 siffer.

2. Sikkerhetspolicy for Mac-enheter

Nr.	Sikkerhetspolicy	Informasjon
1	**Aktivert antivirus**	Sikre integriteten til filstrukturen mot skadelig programvare og uautorisert tilgang.
2	**Aktivering av brannmur**	Begrense uautorisert nettverkstilgang og beskytte enheten mot potensielle trusler utenfra.
3	**Aktivering av kryptering på maskinen**	Beskytte sensitiv bedriftsinformasjon ved å kryptere data på maskinen og forhindre uautorisert tilgang ved tap eller tyveri.
4	**Kontroll av siste aktive sikkerhetsoppdateringer**	Opprettholde en høy sikkerhetsstandard ved å installere kontinuerlige oppdateringer og redusere sårbarheter.
5	**Alltid siste oppdaterte Office-pakke**	Sikre at bedriftens produktivitetsprogramvare er beskyttet mot sårbarheter og utnyttelser.
6	**Automatisk aktivering av låseskjerm etter 5 minutter**	Forhindre uautorisert tilgang når maskinen ikke er i bruk.
7	**Sikker passordpolicy**	Øke sikkerheten ved å implementere sterke passordpraksiser. -Store og små bokstaver. -Siffer -Minst ett spesialtegn -Minimum 8 karakterer Hvis pinkode benyttes, må denne være minimum 6 siffer.

3. Sikkerhetspolicy for Android enheter

Nr.	Sikkerhetspolicy	Informasjon
1	**«Jailbreak»-enheter blir blokkert fra firmaressurser.**	«Jailbreaking» er prosessen med å fjerne begrensningene på en mobil enhet, og det gir brukeren utvidet tilgang og muligheten til å installere ikke-godkjente applikasjoner og modifikasjoner. Stoppe tilgang fra enheter som er «jailbreaket» for å opprettholde integriteten til bedriftens sikkerhetsmiljø.
2	**Kontroll av siste aktive sikkerhetsoppdateringer**	Sikre at enheten har de nyeste sikkerhetsoppdateringene for å redusere sårbarheter.
3	**Kontroll av aktive mobiler med aktiver låsekode**	Øke tilgangssikkerheten ved å påse at alle aktive mobiler har en aktivert låsekode
4	**Kontroll av aktive mobiler med 6-sifret låsekoden**	Styrke låsekodekompleksiteten for å forhindre uautorisert tilgang
5	**Blokkering av apper fra ukjente kilder (ikke Google Play)**	Hindre installasjon av potensielt usikre apper fra kilder utenfor Google Play.
6	**Blokkering av muligheten for USB-hacking**	Beskytte mot potensiell trussel ved å blokkere enhetens mulighet for hacking via USB-porten
7	**Automatisk aktivering av låsekode ved dvalemodus**	Forhindre uautorisert tilgang ved å aktivere låsekode umiddelbart når mobilen går i dvale
8	**Innstilling for automatisk dvalemodus**	Redusere risikoen for uautorisert tilgang ved å sette enheten i dvalemodus automatisk etter en kort inaktivitetsperiode
9	**Påse installasjon av nødvendige apper:**	Sikre at nødvendige bedriftsapper er installert for effektiv kommunikasjon og sikkerhetsadministrasjon. -Outlook -Authenticator -Firmaportal (Intune for mobil)
10	**Datakryptering på enheten**	Beskytte sensitiv informasjon ved å kryptere data lagret på enheten.

4. Sikkerhetspolicy for Android enheter

Nr.	Sikkerhetspolicy	Formål
1	**«Jailbreak»-enheter blir blokkert fra firmaressurser**	«Jailbreaking» er prosessen med å fjerne begrensningene på en mobil enhet, og det gir brukeren utvidet tilgang og muligheten til å installere ikke-godkjente applikasjoner og modifikasjoner. Stoppe tilgang fra enheter som er «jailbreaket» for å opprettholde integriteten til bedriftens sikkerhetsmiljø.
2	**Kontroll av siste aktive sikkerhetsoppdateringer**	Sikre at enheten har de nyeste sikkerhetsoppdateringene for å redusere sårbarheter.
3	**Kontroll av aktive mobiler med aktiver låsekode**	Øke tilgangssikkerheten ved å påse at alle aktive mobiler har en aktivert låsekode
4	**Kontroll av aktive mobiler med 6-sifret låsekoden**	Styrke låsekodekompleksiteten for å forhindre uautorisert tilgang
5	**Automatisk aktivering av låsekode ved dvalemodus**	Forhindre uautorisert tilgang ved å aktivere låsekode umiddelbart når mobilen går i dvale
6	**Innstilling for automatisk dvalemodus**	Redusere risikoen for uautorisert tilgang ved å sette enheten i dvalemodus automatisk etter en kort inaktivitetsperiode
7	**Påse installasjon av nødvendige apper:**	Sikre at nødvendige bedriftsapper er installert for effektiv kommunikasjon og sikkerhetsadministrasjon. -Outlook -Authenticator -Firmaportal (Intune for mobil)

Om sikkerhetspolicy for PC, Mac og mobile enheter

Utgave: **Sikkerhetspolicy for PC, Mac og mobile enheter v2.1**
Endret: **Sist endret 02.02.2024**
Bruksrett: **Tekst og innhold på denne siden kan fritt benyttes og endres som sitt eget dersom bedriften har en kundeavtale med AGS IT-partner.**