# Anbefalt sikkerhetsstandard for bedriften

| Anbefalt standard | Informasjon | NSM Sikkerhetsprinsipp | Aktivert |
|---|---|---|---|
| **Antivirus** | Et antivirusprogram fungerer som en sikkerhetsvakt for datamaskinen. Den overvåker kontinuerlig og hindrer farlige datavirus og skadelige programmer fra å infiltrere maskinen din. | 2.3 - Beskyttelse og opprettholdelse av data<br><br>2.7 - Beskytt data i ro og transitt<br><br>3.1 - Oppdage og fjern kjente sårbarheter og trusler | |
| **To-faktor-autentisering (MFA)** | To-faktor autentisering kan sees på som en ekstra lås på døra til datamaskinen din. Du bruker ikke bare et passord, men også en ekstra kode eller godkjenning. Dette gjør det mye vanskeligere for uvedkommende å få tilgang til dataene dine | 2.2 - Etablere en sikker IKT-arkitektur<br><br>2.4 - Beskytte virksomhetens nettverk<br><br>2.6 - Kontroll på identiteter og tilganger | |
| **Avansert e-post beskyttelse** | Identifiserer kjente trusler og blokkerer, beskytte viktig informasjon, unngå phishing-angrep | 2.8 - Avanserte sikkerhetstiltak for beskyttelse av e-post.<br><br>3.1 Oppdage og fjern kjente sårbarheter og trusler | |
| **Beskyttelse av nettleser** | Identifisere og blokkere potensielle trusler når du besøker nettsteder. | 2.8 - Sikkerhetstiltak for beskyttelse av nettleser.<br><br>3.1 - Oppdage og fjern kjente sårbarheter og trusler | |
| **Kryptering av data på PC og Mac** | Benytter kryptering slik at all informasjon på maskinen gjort uforståelig for de som ikke har tillatelse til å se den | 2.7 - Kryptering som virkemiddel for å beskytte data i ro og i transitt. | |
| **Administrasjon av sikkerhetspolicy på enheter** | En sikkerhetspolicy for bedriftens enheter er et sett med regler og retningslinjer som alle må følge for å holde datasystemet trygt. | 2.6 - Ha kontroll på identiteter og tilganger | |
| **Automatisk sikkerhetsoppdatering** | Automatisk sikkerhetsoppdatering av datamaskiner og programvare uten behov for manuell inngrep fra bruker | 2.3 - Ivareta en sikker konfigurasjon | |
| **Fjernsletting av mistet/stjålet enhet** | Muliggjøre ekstern sletting av all informasjon på en gitt enhet. Dette sikrer bedriftens sensitive data | 2.3 - Ivareta en sikker konfigurasjon | |
| **Sikring mot lekkasje på Darkweb** | Sikrer mot datalekkasje og forhindre identietstyveri og tap av omdømme | 2.3 - Ivareta en sikker konfigurasjon | |
| **Opplæring og testing av ansatte for å øke sikkerhetsbevisstheten** | Opplæring og testing for å øke sikkerhetsbevisstheten hos ansatte er viktig for å styrke organisasjonens overordnede sikkerhetskultur, redusere risikoen for menneskelige feil, og skape et felles ansvar for datasikkerhet blant de ansatte. | 3.4 - Gjennomfør inntrengingstester<br><br>4.4 - Evaluer og lær av hendelser | |

| | | | |
|---|---|---|---|
| **Sårbarhetsanalyse** | Analysere og finne sårbarheter på enheter, programvare, nettverk og systemer som kan benyttes til et dataangrep. | 2.3 - Ivareta en sikker konfigurasjon<br>3.1 Oppdage og fjern kjente sårbarheter og trusler | |
| **Etabler system for monitorering Internt eller eksternt (SOC)** | Etablering av et system for monitorering av bedriftens datapark (Security Operation Center) er avgjørende for å styrke organisasjonens IT-sikkerhet. | 3.2 - Etabler sikkerhets overvåkning<br><br>3.4 - Analyser data fra sikkerhets- overvåkning<br><br>4.1 - Forbered virksomheten på håndtering av hendelser<br><br>4.2 - Vurder og klassifiser hendelser<br><br>4.3 - Kontroller og håndter hendelser | |
| **Sikkerhetskopiering av data**<br><br>**(a) Backup av lokale IT-ressurser**<br><br>**(b) Backup av skybaserte IT-tjenester** | Plan for sikring av data gjennom regelmessig sikkerhetskopiering er avgjørende for å beskytte seg mot tap av informasjon, og for å sikre rask gjenoppretting i tilfelle uønskede hendelser | 2.9 - Etabler evne for gjenoppretting av data | |
| **Sikker gjenbruk/resirkulering av IKT-utstyr** | Det er viktig å ha på plass rutiner for at konfidensiell data blir slettet fra enhetene bedriften kvitter seg med. | 2.2 - Etablere en sikker IKT-arkitektur<br><br>2.7 - Beskytt data i ro og transitt | |
| **Generell sikkerhetspolicy for ansatte i bedrifte** | Implementering av IT-policyer er avgjørende for å sikre en robust og trygg digital arbeidsplattform for ansatte<br>Se vedlegg | 2.2 - Etablere en sikker IKT-arkitektur | |
| **Enhetsbasert sikkerhetspolicy** | Spesifikke retningslinjer som adresserer sikkerhetsaspekter knyttet til bruk av enhetene i bedriften<br>Se vedlegg | 2.2 - Etablere en sikker IKT-arkitektur | |
| **Kartlegg styringsstrukturer, leveranser og understøttende systeme** | Virksomheten bør kartlegge risiko og sikkerhet for sine understøttende systemer | 1.1 - Kartlegge styringsstrukturer, leveranser og understøttende systeme | |
| **Kartlegg enheter og programvarer** | Virksomheten bør kartlegge enheter og programvare på nettverket for å ha oversikt over forvaltede (og ikke-forvaltede) enheter og gjeldende konfigurasjon for disse. | 1.2 - Kartlegge enheter og programvare | |
| **Kartlegg brukere og behov for tilgang** | Virksomheten bør skaffe oversikt over hvilke brukergrupper, brukere og tilgangsbehov som finnes i virksomheten og har kartlagt ansvar for IKT-sikkerhet. | 1.3 Kartlegge brukere og behov for tilgang | |
| **Sikkerhetsavtale** | Grunnleggende avtale for ansvar og håndtering av sikkerheten i bedriften<br>Se vedlegg | 4.1 - Forbered virksomheten på håndtering av hendelser | |

**Utgave**: v2.1 **Sist endret**:  05.02.2024