Nettsoft sikkerhetsløsninger

Følgende viser en oversikt over sikkerhetstiltak og tjenester som anbefales innført i bedriften.
Dersom bedriften benytter Microsoft 365 finner du egne anbefalinger for dette fra side 4.

Tiltak består i hovedsak av engangarbeid, mens tjenester omfatter løpende abonnementer. Priser oppgis i tilbud.

Nettsoft Nødplakat for Digitale Angrep	Last ned nødplakat for kontoret
Godkjenne E-post/domenebeskyttelse	For å forhindre at bedriftens e-post domenenavn benyttes til spam og svindel (spoofing), og for å sikre at e-post du sender ikke blir sperret av mottakerens e-post server, må det gjøres tilpassinger på domenenivå. Les en oppsummering av funksjonaliteten her. **Tiltak:** Vi kontrollerer og gjør nødvendige tilpasninger på domenet (og eventuelt M365).
Beskyttelse av lokalt nettverk (internettlinje)	For å beskytte bedriftens nettverk og utstyr, anbefaler vi at det først og fremst aktiveres sikkerhetstjenester fra din internett leverandør. Slike tjenester stopper kjente trusler før det når lokalt nettverksutstyr og ansattes maskiner. En fordel med å benytte sikkerhetstjenester hos din internettleverandør, er at det ikke reduserer hastigheten på din internettforbindelse. Se video om SafeZone hos Telenor (YouTube) Les mer om SafeSurf hos GlobalConnect **Tiltak/tjeneste:** Vi undersøker om/hvilke sikkerhetstjenester som er tilgjengelig hos din Internettleverandør.
Beskyttelse av datamaskiner	1. BITLOCKER: Datakryptering (inkludert i Windows) 2. CYBERSIKKERHET: SentinelOne EDR, for å beskytte mot sanntid cyberangrep, skadelig programvare og (løsepenge)virus. Systemovervåkning og enklere fjernhjelp fra Nettsoft. 3. WINDOWS 11 Etter 14.oktober 2025 mottar ikke maskiner med Windows 10 **Pro** oppdateringer fra Microsoft. **SentinelOne EDR:** Abonnementstjeneste betalt per enhet per måned. Tjenestebeskrivelse og vilkår

Post- og besøksadresse:
Strømsveien 223
0668 OSLO

Kontaktinformasjon:
info@nettsoft.no
nettsoft.no/kontakt

Hovednummer:
+47 22 88 19 19

Microsoft Teams
ansattfornavn@nettsoft.no

Beskyttelse av mobile enheter	1. Aktivert biometrisk pålogging (Face-ID/fingeravtrykk) 2. Ikke bruke offentlig WiFi uten VPN fra mobiloperatør. 3. Ved bruk av M365, benytt MAM eller MDM for å sikre bedriftsdata. Se eget kapittel under M365. Se video om SafeZone hos Telenor (YouTube) **Tiltak/tjeneste:** Avhengig av behov og valg av tjenester.
Oppdatering av lokal infrastruktur og utstyr *Nettverk driftsavtale*	Sørge for at alt av nettverksutstyr alltid inneholder siste programvare og sikkerhetsfunksjoner. Vi anbefaler at utstyret inngår i vår nettverk driftsavtale, slik at vi enklere og periodisk kan kontrollere utstyret. **Tiltak/tjeneste:** Nettverk driftsavtale er en tjeneste betalt per enhet per mnd. Tjenestebeskrivelse og vilkår
Backup/Sikkerhetskopiering	Backup er viktig for å hindre tap av data ved kompromittering, datafeil, eller tap av maskiner. *OBS! OneDrive/SharePoint og andre fillagringstjenester er ikke en backupløsning da kompromitterte data kan spre seg i bedriften.* Vi til tilbyr markedsledende backuptjenester og utstyr fra blant annet Cove Data Protection™ og Synology™. Vi kan også levere hybrid backup ved bruk av lokal lagringsenhet (nettverksdisk/NAS), dersom du ønsker tilgang til dine data om Internett ikke fungerer. Se eget kapittel.
Sikkerhetskurs for ansatte (fysisk eller webinar)	Menneskelige feil fører til flest alvorlige sikkerhetsbrudd. Økt kunnskap er derfor viktig. Vi holder kurs for ansatte, og går igjennom fordeler og ulemper med valg av utstyr og løsninger, passordhåndtering, netthandel mv. Vi fokuserer på kjente svindelmetoder og sosial manipulasjon. Kurset tar én – to timer avhengig av spørsmål, og kan avholdes fysisk eller via Teams. Etter kurset mottar deltagere informasjon for å holde seg oppdatert på IT-sikkerhet. Tjenestebeskrivelse
Beredskapsplan	IT-angrep skjer når du minst venter det. Beredskapsplan er HMS, og viktig for å ha kontroll og oversikt over egne data, og hvilke prosedyrer som skal følges i tilfelle sikkerhetsbrudd, feil eller tap av utstyr. **Tiltak:** Vi lager en plan basert på de tjenestene bedriften benytter. Tjenestebeskrivelse

Hybrid backup, lokal fillagring og samarbeid (NAS)

Nasjonal Sikkerhetsmyndighet (NSM) anbefaler at bedrifter har tilgang til kritiske data lokalt, i tilfelle bortfall av Internett og skytjenester.

Vi tilbyr løsninger som gjør det mulig å lagre backup både i skyen og på lokal nettverksdisk, kalt NAS (Network Attached Storage). Kort sagt vil en NAS kunne sørge for at deres data er tilgjengelig selv ved utfall av Internett og skytjenester.

En NAS kan også ta backup av M365, og tilbyr i tillegg en rekke tjenester for blant annet backup av bilder fra ansattes mobile enheter, filsynkroniseringstjenester (tilsvarende OneDrive, Dropbox), dokumenthåndtering, e-post tjenester mm. Alt du har lagret på NAS-en kan i tillegg kjøre backup til ekstern leverandør for enda flere lag med beskyttelse.

Sikring og overvåkning av kontorer, lager mm.

For å hindre uvedkommende adgang til bedriftens datautstyr, er det det smart og preventivt å ha kontroll på sine lokaler og utstyr.

For bedrifter underlagt NIS/NIS2 påkrevet å ha fysisk og elektronisk sikring av adgang.

Nettsoft er autorisert forhandler av Elotec Ajax, som er det mest prisbelønte, profesjonelle alarmsystemet i Europa, og eneste norske alarmsystemet som har felles FG-godkjenning innenfor brann, vann, innbrudd og lås (grad 2).

Ajax har en overlegen rekkevidde og sikkerhet, og har produkter og løsninger som ikke kan leveres av andre alarmsystemer.

Ajax leverer også (NDAA) godkjent videoovervåkningsutstyr. Alt samlet i ett system du eier og kan overvåke selv uten månedskostnad, eller koble til et av flere alarmselskap, herunder Securitas, Avern, Sikring24 m.fl.

Ajax systemet består av (FG) forsikring-, TEK-17 og Sintef godkjente, profesjonelle kvalitetsprodukter, med unike løsninger innen objektsikring og styringssystemer til boliger og hytter, næringsbygg og butikker, og til leilighetsbygg og borettslag/sameier.

Vi samarbeider med låsesmeder og andre fagområder for totalsikring.

Krisehåndtering og utvidet testing av utstyr og ansatte

Dersom du mistenker at utstyr eller data er under angrep, er det viktig at du kontakter oss så snart som mulig. Avhengig av angrepets omfang vil vi sette i gang tiltak for å redusere skaden og beskytte data.

Vi samarbeider med det norsk sikkerhetsselskapet Fence for eventuell bistand ved større, alvorlige angrep. Fence leverer også tjenester for å teste bedriftens datautstyr og ansattes håndtering av data (bl.a. e-post pishing test).

Tjenester fra vår samarbeidspartner fence.no	• ROS (Risiko Og Sårbarhetsanalyse) • Phishing test (periodisk e-post test av ansatte) • Pentesting / Sikkerhetstesting • 24/7 sikkerhetssupport

Post- og besøksadresse:
Strømsveien 223
0668 OSLO

Kontaktinformasjon:
info@nettsoft.no
nettsoft.no/kontakt

Hovednummer:
+47 22 88 19 19

Microsoft Teams
ansattfornavn@nettsoft.no

Microsoft 365 (M365)

M365 er bedriftens plattform for kommunikasjon, lagring og utveksling av data. Det er derfor spesielt viktig at disse tjenestene blir beskyttet best mulig.

M365 inneholder en rekke innebygde sikkerhetsfunksjoner, men disse må aktiveres og tilpasses. Tilgjengelige sikkerhetsfunksjoner er avhengig av hvilke lisenser (planer) bedriften benytter.

Ved å la Nettsoft administrere bedriftens M365 lisenser er det enklere å kontrollere at bedriften benytter riktige lisenser ift. sikkerhet og funksjonalitet. Vår tjeneste for **lisensadministrasjon** inkluderer brukersupport for ansatte.

Tiltak består i hovedsak av engangarbeid, mens tjenester omfatter løpende abonnementer. Priser oppgis i tilbud.

Obligatorisk to-faktor pålogging (MFA)	To-faktor pålogging bidrar til å forhindre tilgang til kontoer med kun brukernavn og passord, og gir et ekstra lag med beskyttelse ved å be om en ekstra kode/passnøkkel for å bekrefte identiteten din. **Tiltak:** Funksjonen er inkludert i alle M365 abonnement, men må aktiveres og tilpasses, slik at den blir obligatorisk.
Kontrollere tilgangsnivå for ansatte	Ingen ansatte eller ledelse bør ha global administratortilgang til M365, ettersom en slik konto har rettigheter til å endre alle innstillinger, passord på ansatte, og slå av sikkerhetsfunksjoner, **Tiltak:** Vi kontrollerer tilgangsnivået, og avtaler nødkonto.
Logging av hendelser (Audit)	Dersom det oppstår et sikkerhetsbrudd, er det som standard kun mulig å sjekke aktiviteter/logger 7 dager bakover i tid. Ved å aktivere funksjonen «Audit» er det mulig å hente ut logger på inntil 180 dager. Funksjonen er inkludert i M365. **Tiltak:** Aktivering i M365
M365 Backup	Selv om bedriftens data er lagret i M365 (skyen) er ikke dette en backup-løsning dersom det skulle oppstå datafeil, eller dataene blir kapret eller angrepet av løsepengevirus, som krypterer alle dataene. Vi tilbyr både ekstern og lokal hybrid backup av M365 data. Se også kap. om NAS. Tjenestebeskrivelse: Backup MS365 | Hybrid NAS
Nettsoft Kontovakt for M365	Kontovakt er Nettsoft utviklet M365 app (Entra/Graph-API integrasjon), som bidrar til å avsløre kontokapringer ved å rapportere mistenkelige påloggінger og endringer i e-post regler, som ofte benyttes av kriminelle. Tjenestebeskrivelse og avtalevilkår: Nettsoft Kontovakt
Supportavtale brukere	For raskere bistand til ansatte Tjenesten er inkludert ved Nettsoft lisensadministrasjon. Tjenestebeskrivelse og avtalevilkår: Support M365 Bruker
Supportavtale Bedrift	For bistand til administrasjon av M365 på bedriftsnivå Tjenestebeskrivelse og avtalevilkår: Support M365 Bedrift

Post- og besøksadresse:
Strømsveien 223
0668 OSLO

Kontaktinformasjon:
info@nettsoft.no
nettsoft.no/kontakt

Hovednummer:
+47 22 88 19 19

Microsoft Teams
ansattfornavn@nettsoft.no

Lisenskrav: Business Premium og/eller Entra P1 og Defender P1	
Tilgangskontroll	For å forhindre at uvedkommende/kriminelle kan logge seg på M365 er det to metoder som kan benyttes: 1. **Enhetsstyrt pålogging** Dette er en funksjon som gjør at kun godkjente maskiner kan logge seg på og få tilgang til M365. Maskinene må være innmeldt i Entra (Azure). 2. **Regionspålogging** Dette er en funksjon som kan forhindre pålogging fra land som ikke er forhåndsgodkjent. Kan benyttes for alle enheter, uavhengig av om de er meldt inn i Entra (Azure). **Tiltak:** Aktivering i M365. **Tjeneste:** Supportavtale for regionspålogging.

Lisenskrav: Business Premium og/eller Entra P1 og Defender P1	
Mobil enhetskontroll (MAM/MDM)	For å kontrollere at kun mobile enheter som oppfyller krav til bruk av kode, passord og biometri får tilgang til M365, og å muliggjøre fjernsletting (Wipe) av tapte enheter, er det to metoder som kan benyttes. 1. **MAM (Mobile Application Management)** Funksjon for å administrere og sikre tilgang til M365 Apper, uten å administrere hele enheten. Passer for mobile enheter som også benyttes personlig (BYOD). 2. **MDM (Mobile Device Management)** Funksjonen for å kontrollere alt på mobile enheter. Passer best for mobile enheter som kun brukes i jobb. *Android enheter må i tillegg benytte M365 bedriftsportal.* **Tiltak:** Aktivering avhengig av valgt tjeneste i M365 **Tjeneste:** Supportavtale for MDM.

Lisenskrav: Business Premium og/eller Entra P2 og Defender P2	
M365 sikkerhetsanalyse	M365 funksjon som automatisk analyserer og rapporterer mistenkelig brukeradferd.