

Komplett produktinfo om Kirkens lokale skrivebord

Kirkens lokale skrivebord (KLS) er en ferdig oppsatt og driftet Microsoft 365-installasjon (tenant), spesielt tilpasset behovene til Den norske kirke. Den har et omfattende sett av verktøy og applikasjoner som inkluderer Microsoft 365-applikasjoner og Microsoft Intune, som muliggjør enkel og sikker administrasjon av alle enhetene som brukes med KLS i kirken.

Miljøet er satt opp med sikkerhetspolicyer i henhold til anbefalinger fra Microsoft, Sikkerhetsutvalget i Den norske kirke og systemeier i Kirkerådet. Dette gir en rekke fordeler for Den norske kirke. For det første sikrer det at all data og informasjon som behandles av kirken, er godt beskyttet mot uautorisert tilgang og misbruk, noe som er spesielt viktig med tanke på økende trusler fra cyberkriminalitet.

I tillegg til å beskytte dataene, gir Kirkens lokale skrivebord enkel og effektiv tilgang til blant annet Teams, SharePoint og OneDrive, som gjør det enkelt å samarbeide og dele informasjon på tvers av enheter og geografiske lokasjoner.

Tjenesten inkluderer også Single-Sign-on (SSO) mot fellesløsninger i Den norske kirke, noe som forenkler og forbedrer brukeropplevelsen ved å gi brukerne muligheten til å logge på én gang og få tilgang til flere applikasjoner uten å måtte huske separate brukernavn og passord for hver applikasjon.

Kirkens lokale skrivebord har kalenderintegrasjon med fagsystemene fra Vitec Agrando og Kirkeidata. KLS har også integrasjon med kirkens fellesløsning for sak-, arkiv- og møte Dnk360 (basert på Public 360 fra Tieto), noe som kan føre til økt effektivitet og nøyaktighet i arbeidsprosessene ved å automatisere dataflyt mellom forskjellige applikasjoner og fagsystemer. Integrasjonen med SSO kan gi en sømløs og mer effektiv arbeidsflyt for de ansatte i kirken. Det ferdig oppsatte og driftede miljøet frigjør ressurser som kan brukes til å styrke kirkens primære oppgaver og formål.

Miljøet inneholder en omfattende sikkerhetspakke med Microsoft 365 E3 + E5 Security lisensnivå, sikkerhetsovervåkning, e-postbeskyttelse mot farlige lenker og vedlegg, sikker 2-trinns-pålogging, kryptering av PC mot tyveri og uhell, nettfiler for sikker surfing på internett, sikker print, identitetsportal for bruker- og tilgangsstyring, samt sikkerhetsoppdateringer.

2.1 Komponenter i Kirkens lokale skrivebord

2.1.1 Microsoft 365 lisens (Microsoft E3)

Microsoft 365 lisens (Microsoft E3) er en samling av produktivitetsverktøy og enkle sikkerhetsløsninger som er spesielt utviklet for å møte behovene til bedrifter og organisasjoner i ulike størrelser og bransjer.

Microsoft Office 365 Pro Plus gir fullverdige desktopløsninger for produktivitet og samarbeid med kjente programmer som Word, Excel, PowerPoint, Outlook og OneNote. I tillegg er også Access og Publisher tilgjengelig på forespørsel.

Microsoft Exchange Online er en skybasert e-postløsning som gir bedrifter og organisasjoner sikker tilgang til e-post, kalender og kontakter fra hvor som helst og når som helst.

Microsoft Teams: Teams er en kommunikasjons- og samarbeidsplattform som gir en rekke funksjoner som chat, videosamtaler, skjermdeling, fil- og applikasjonsdeling og mer. Teams gir Den norske kirke muligheten til å samarbeide på tvers av enheter og lokasjoner, og kommunisere med medarbeidere og andre interessenter på en sikker måte. Teams fungerer også som en plattform for virtuelle møter, konferanser og arrangementer.

SharePoint: SharePoint er en skybasert plattform for dokumenthåndtering og lagring, og er det felles lagringsområder i Kirkens MS365-område. Administrasjon av felles dokumenter gjøres enklest gjennom Teams. Via Teams-rom kan man opprette og dele dokumenter. Teams er bygget på SharePoint sin filstruktur, og oppretter du et Teams-rom oppretter du automatisk et mappeområde i SharePoint. [Kirkens informasjonsveileder](#) beskriver nærmere hvordan Teams bør være det foretrukne inngangsportalen til filer som ligger i SharePoint.

OneDrive: OneDrive er en skybasert lagringstjeneste som gir mulighet til å lagre, synkronisere og dele filer og mapper på tvers av enheter og plattformer. Som en del av Office 365-abonnementet, får brukere i Den norske kirke tilgang til god lagringsplass i OneDrive. Dette gjør det enkelt å lagre og dele dokumenter og annen informasjon med andre i organisasjonen, uansett hvor de befinner seg. OneDrive gir også mulighet til å arbeide offline og synkronisere endringer med skyen når man er tilkoblet igjen.

Alle disse verktøyene kan bidra til å forbedre samarbeidet og produktiviteten for Den norske kirke, samt gjøre det enklere å dele informasjon og samarbeide. Pakken inneholder også løsninger som Bookings, Planner, Stream, Project for Office, To-Do, med mer.

2.1.2 Sikkerhetspakken (Microsoft E5 Security)

Sikkerhetspakken inkluderer en rekke avanserte sikkerhetsfunksjoner som gir ekstra beskyttelse for kirkens data og brukere og gir brukere av Kirkens lokale skrivebord et samlet førstelinjeforsvar mot sikkerhetstruslene som finnes i dagens digitale miljø, med muligheten til å håndtere dem på en effektiv måte. Plattformen gir også enkel integrasjon med eksisterende infrastruktur og verktøy, og gir en helhetlig sikkerhetsløsning for Den norske kirke. Oppsettet bygger sikkerhetsbarrierer via Microsoft Defender-suiten og er en integrert sikkerhetsplattform i Kirkens lokale skrivebord. Plattformen gir beskyttelse mot en rekke trusler, inkludert skadelig programvare, phishingangrep, avanserte trusler og datasikkerhetshendelser. Her er en oversikt over hva som er inkludert og konfigurert som en del av Kirkens lokale skrivebord:

Microsoft Defender for Endpoint:	En avansert beskyttelsesplattform som gir endepunktsikkerhet, angrepsdeteksjon og responsfunksjoner, samt beskyttelse mot skadelig programvare, phishingangrep og annen truende aktivitet.
Azure Advanced Threat Protection:	En tjeneste for å oppdage og beskytte mot avanserte trusler som kan angripe nettverket, inkludert bruk av maskinlæring for å analysere brukeratferd og avdekke avvik.

Azure Active Directory Premium P2:	En identitets- og tilgangskontrolltjeneste som gir ekstra funksjoner for beskyttelse av identiteter og tilgangskontroll, inkludert adaptive autentiseringsmetoder og risikobasert tilgang.
Office 365 Advanced Threat Protection:	En tjeneste for å beskytte mot avanserte trusler i e-post, inkludert beskyttelse mot skadelig programvare og phishingangrep.
Microsoft Cloud App Security:	En tjeneste for å beskytte mot skybaserte sikkerhetsrisikoer, inkludert identitets- og tilgangskontroll, beskyttelse av data og trusselbeskyttelse.
Microsoft Defender for Identity	En tjeneste for å oppdage og beskytte mot identitetsbaserte trusler og angrep, inkludert overvåking av identitets- og tilgangskontrollaktivitet og deteksjon av ondsinnet bruk av kontoer.

Sikkerhetspakken på Kirkens lokale skrivebord overvåker følgende for å sikre trygg bruk av Microsoft 365:

Passordmonitorering: Vi overvåker brukerens passord og varsler umiddelbart hvis det er lekket eller kompromittert.

Mistenkelige innlogginger: Vi holder øye med innlogginger fra andre land som kan være mistenkelige og potensielt skadelige.

ThreatMap: Vår trusselanalyse gir sanntidsinformasjon om aktiviteter og vellykkede/mislykkede angrep på Microsoft 365-kontoer fra andre land.

Microsoft Defender for Business: Vi bruker data fra Microsoft Defender for Business i Kirkens lokale skrivebord for å oppdage malware, virus, cryptolocker, ransomware, farlige e-post-lenker og vedlegg.

Kontinuerlig monitorering og logging: Vi overvåker og logger aktivitet i Microsoft 365-miljøet kontinuerlig.

Sårbarhetsdeteksjon: Vi oppdager sårbarheter og risikoutsatte kontoer og gir deg beskjed om eventuelle trusler.

Automatisk varsling og sakshåndtering: Hvis det oppdages alvorlige datainnbrudd eller cyberangrep, vil systemet automatisk opprette en sak for å håndtere problemet.

Automatisk isolasjon av klienten: Hvis klientmaskinen blir utsatt for et angrep eller blir kompromittert, vil systemet automatisk isolere maskinen. Vi vil gjenåpne klientmaskinen innenfor gjeldende SLA, og etter at hendelsen er sjekket ut.

Vi tar sikkerhet på alvor og jobber kontinuerlig for å beskytte dine data og din brukeropplevelse i Kirkens lokale skrivebord.

Sikkerhetspakken gir beskyttelse mot mange trusler, men gir samtidig ingen garanti mot angrep. [Samarbeidsavtalen](#) mellom Kirkepartner og Kirkerådet beskriver vilkår ved angrepstilfeller. Sikkerheten påvirkes også av sluttbrukers aktsomhet og kan økes ved å ta [kurs i personvern og informasjonssikkerhet](#). Sluttbruker plikter å følge retningslinjer vedtatt av kirkens Sikkerhetsutvalg for personvern og informasjonssikkerhet.

2.1.3 Support og drift

Support og drift med Kirkepartner Servicedesk er en IT-supporttjeneste som er spesielt tilpasset behovene til Den norske kirke og er det sentrale knutepunktet for henvendelser fra brukere med Kirkens lokale skrivebord. Servicedesk er bemannet med erfarne IT-konsulenter som kan hjelpe ansatte og frivillige i Den norske kirke med tekniske problemer og spørsmål. Servicedesk behandler henvendelser fra brukere, feilsøker problemer og gir veiledning for å hjelpe brukerne med å bruke teknologi effektivt.

2.1.4 ID-web

ID-web, kjent som Microsoft Identity Manager (MIM) i andre sammenhenger, er Den norske kirkes identitets- og tilgangsstyringsløsning for administrasjon av brukere og rettigheter til flere av kirkens fellesløsninger. MIM, eller ID-web som det kalles internt i kirken, gir en sentralisert plattform for å opprette, administrere og synkronisere brukerprofiler og tilgangsrettigheter på tvers av forskjellige applikasjoner og systemer som brukes av kirken.

ID-web, fungerer som en identitetsdatabase som muliggjør opprettelse og vedlikehold av brukerprofiler for kirkens ansatte, frivillige og andre som trenger tilgang til kirkens IT-ressurser. Hver brukerprofil kan inneholde relevante attributter som navn, adresse, kontaktinformasjon og annen identitetsrelatert informasjon.

Ved hjelp av ID-web, kan Den norske kirke også definere og administrere tilgangsrettigheter for hver bruker basert på deres rolle og ansvarsområde. Dette inkluderer bestemmelse av hvilke IT-systemer og applikasjoner en bruker har tilgang til, samt hvilke funksjoner og data de kan håndtere innenfor disse systemene. Ved å tildele passende rettigheter sikrer kirken at brukerne bare har tilgang til de nødvendige ressursene for å utføre sine oppgaver.

ID-web er integrert med bruker- og identitetssystemer som Active Directory og Azure AD.

2.1.5 Brukerstøtte

Kirkepartner Servicedesk tilbyr support via telefon, e-post eller chat, avhengig av hva som passer best for den enkelte bruker. Det finnes også en selvhjelpsportal. Tjenesten er tilgjengelig fra mandag til fredag i normal kontortid og inkluderer blant annet:

- Hjelp med å sette opp og konfigurere Kirkens lokale skrivebord på datamaskiner og telefoner.
- Feilsøking og retting av feil som oppstår i produktporteføljen tilknyttet KLS.
- Støtte for Microsoft Office og andre fellesløsninger for Den norske kirke.
- Hjelp med å administrere brukerkontoer og tilgang via ID-web.
- Hjelp med å opprettholde sikkerhet og beskytte systemene mot trusler.
- Fjernstyre brukerens enhet ved behov og samtykke.
- Ved innmeldt tyveri, fjernsletter også Kirkepartner Servicedesk innholdet på mobile enheter.
- Vedlikeholder selvhjelpsportal med Ofte Stilte Spørsmål (OSS/FAQ) og manualer på <https://sd.kirkepartner.no>

Normalt er Servicedesk åpent man-fre 07:30-16:30, med noen avvikende åpningstider rundt helligdager. Alle saker registreres for oppfølging og rapportering.

Se [Samarbeidsavtalen](#) mellom Kirkepartner og Kirkerådet for Service Level Agreement (SLA).

De fleste samtaler besvares innen 3 minutter, og varer normalt i 6-8 minutter. Ved uforutsette «bølger» på telefon vil svartiden i noen tilfeller øke utover 10 minutter. Innringer tilbys tilbakering ved lengre køtider.

Brukere med behov for kompetanseheving henvises til ressurser for opplæring og kursing ved antatt behov for hjelp ut over 20 minutter.

Feil på pc-er og mobile enheter må vurderes rettet gjennom resett av enheten dersom det antas at feilretting vil ta mer enn 30 minutter.

Ved mye kø på servicedesk kan man avtale tilbakering på et tidspunkt med ledig kapasitet for å forhindre lang svartid.

2.1.6 Opplæring

Systemeier i Kirkerådet har ansvar for opplæringsmaterieil i form av videoer, veiledninger og webinarer. Dette utvikles basert på brukerens behov og finnes på Ressursbanken og Kirkens læringsplattform. Sluttkunde kan bestille online-opplæring eller klasseromskurs i bruk av Kirkens lokale skrivebord fra Kirkepartner. Dette faktureres sluttkunde etter avtale / bestilling.

2.1.7 Klientdrift

Klientdrift med Microsoft Intune gir mulighet for å utføre klientdrift av en PC-park ved å administrere enhetene sentralt fra en portal, uavhengig av hvor enhetene befinner seg. Dette kan omfatte ulike oppgaver, som for eksempel:

Overvåkning og administrasjon av enhetskonfigurasjoner: Med Intune kan man sentralt administrere enhetskonfigurasjoner på tvers av ulike operativsystemer, inkludert Windows. Dette kan omfatte konfigurasjon av sikkerhetsinnstillinger, nettverksinnstillinger, applikasjoner og programvareoppdateringer. Distribusjon av programvareoppdateringer og patching: Intune gir mulighet for å distribuere programvareoppdateringer og patching på tvers av enhetene i organisasjonen, som bidrar til å holde enhetene oppdatert og beskyttet mot sikkerhetstrusler.

Enhetsstyring og sikkerhet: Intune gir mulighet for å administrere sikkerhetsinnstillinger på enhetene, som passordbeskyttelse, fjernsletting av data på tapte eller stjålne enheter, og krav om oppdatering til siste versjon av operativsystemet. Overvåkning av enheter og rapportering av problemer: Intune gir mulighet for overvåkning av enhetene i sanntid, og rapportering av problemer for å identifisere og håndtere problemer så raskt som mulig.

Til sammen gir Intune en rekke funksjoner og verktøy for administrasjon av enheter og applikasjoner i en PC-park. Dette gjør det enklere å administrere og sikre enhetene i organisasjonen, samtidig som man kan få bedre kontroll over enhetskonfigurasjoner og kostnader.

Intune tilbyr flere funksjoner som hjelper Kirkepartner med å administrere og sikre enhetene i Den norske kirke som benytter Kirkens lokale skrivebord. Blant annet kan Intune automatisk rulle ut nødvendige applikasjoner til brukerne og Kirkepartner kan administrere og kontrollere sikkerhetsnivået på alle enheter, inkludert mobile enheter.

Systemeier i Kirkerådet og Kirkepartner har definert en felles sikkerhetspolicy som alle enheter må oppfylle, og dette sikrer at alle enhetene etterfølger Microsofts beste praksis for sikkerhet. I tillegg til å kunne fjernslette enheter som blir stjålet, mistet eller offboardet, tilbyr Klientdrift av Kirkens lokale skrivebord også muligheten til å separere kirkens data fra private data på enhetene.

2.1.8 Sikker print

Inkludert i Kirkens lokale skrivebord er en skybasert printløsning som gjør det enkelt å skrive ut dokumenter fra ulike enheter og steder. Sikker print tilbyr funksjonalitet for automatisk skriverinstallasjon, sikker utskrift, og rapportering av printaktivitet.

Sikker print er viktig for å beskytte organisasjonsdata og hindre uautorisert tilgang til sensitive dokumenter. Sikker print er også viktig for å redusere printkostnader, ved å hindre uønsket utskrift og unødvendig bruk av papir og blekk. Printix tilbyr også funksjonalitet for automatisk skriverinstallasjon, som gjør det enkelt for brukere å sette opp og koble til skrivere, uavhengig av hvilket av arbeidsplassens kontor de befinner seg. Dette gjør det enkelt å skrive ut dokumenter fra ulike enheter og steder, samtidig som sikkerheten opprettholdes.

2.1.9 Døgnskategorisk overvåking og respons

Døgnskategorisk overvåking og respons av sikkerhetstrusler mot Kirkens lokale skrivebord via logger fra klientdrift og Microsoft Sentinel gir Den norske kirke en omfattende og avansert løsning for overvåking og beskyttelse. Med Intune kan administreres sikkerhetspolicyer på enhetene, og med Sentinel overvåkes loggdata og trusler i sanntid.

Fordelene med å bruke en slik løsning:

- Kontinuerlig overvåking av enhetene og nettverket.
- Sanntidsdeteksjon av sikkerhetstrusler.
- Rask respons på sikkerhetshendelser.
- Sentralisert administrasjon av enheter og sikkerhetspolicyer.
- Avansert teknologi og ekspertise for å beskytte organisasjonen.
- Redusert risiko for sikkerhetsbrudd og datatap.

Dette utgjør grunnlaget for Kirkepartners Sikkerhetsoperasjonssenter (SOC) som samler inn store mengder loggdata for å avdekke unormal oppførsel eller trusler imot kirkens IKT-miljø.

Når en sikkerhetshendelse oppdages, vil Kirkepartner umiddelbart iverksette tiltak for å begrense skaden. Dette kan inkludere å isolere berørte systemer fra nettverket, undersøke hendelsen for å fastslå omfanget og arten av trusselen, og iverksette tiltak for å hindre at hendelsen gjentar seg. Det opprettes også kontakt med brukeren i de tilfeller der dette er mulig og formålstjenlig.

En døgnbemannet SOC er avgjørende for Den norske kirke som ønsker å beskytte sine IT-systemer og data mot stadig mer sofistikerte og avanserte trusler. Ved å ha eksperter som er tilgjengelige hele døgnet for å overvåke, analysere og respondere på sikkerhetshendelser, kan kirken reagere raskt og effektivt på trusler og minimere skadeomfanget i et stadig mer sikkerhetsutsatt digitalt trusselbilde.

2.1.10 Backup av Microsoft 365

Selv om Microsoft 365 leverer en solid plattform for å lagre og administrere data i skyen, kan det fortsatt være risiko for uventede hendelser som kan føre til tap av data. Backup-tjenesten gir en ekstra sikkerhetskopii av dataene som er lagret i Microsoft 365, som gir ekstra beskyttelse mot tap av data.

Backup-tjenesten gjør det mulig å ta sikkerhetskopi av all data som er lagret i Microsoft 365, inkludert e-poster, dokumenter, kalendere, kontakter og mer. Sikkerhetskopieringen kjøres automatisk på planlagte tider, og inkluderer også arkivering av data for etterlevelse av regelverk. Sikkerhetskopiene som tas, krypteres og lagres på et sikkert sted, adskilt fra den primære lagringen i Microsoft 365. Dette gir en ekstra sikkerhet mot datatap som følge av for eksempel malware-angrep, menneskelig feil eller brudd på integritet i løsningen. Gjenoppretting av data fra backup testes minimum en gang hvert år. Ved å benytte backup-tjenesten kan Den norske kirke være trygg på at kirkens data er sikret og beskyttet mot tap. Tjenesten gir også mulighet for rask gjenoppretting av data, som kan redusere nedetid og øke produktiviteten i organisasjonen.