

# IKT-Kravspesifikasjon

## Eksisterende IKT-plattform og nettverk

Harstad kommune har etablert et felles nettverk for alle kommunens lokasjoner og Harstad havn sine lokasjoner, totalt har Harstad kommune ca. 240 lokasjoner på nett. Vårt nettverk er bærer av alle IKT-tjenester og internett fra vårt serverrom som er lokalisert på Rådhuset.

Harstad kommune har to rådhus, 1 og 2, vi har backup i rådhus 2 og jobber med en ekstra Site 2-løsning lokalisert i Rådhus 2, samt nytt datasenter i nytt Helsehus som står ferdig i 2025.

Utelokasjoner benytter egen brannmur som IKT-tjenesten leverer og drifter, en såkalt SD-WAN løsning. Det er egne lag3 nett og VPN-benyttes for sikker forbindelse inn til datasenteret sentralt.

Utelokasjoner snakker ikke med hverandre med mindre det er spesifisert og kreves i leveransen.

Vi benytter desentralisert WIFI-løsning med WIFI-kontrollere i brannmurer pr lokasjon, for redundans og sikkerhet.

Harstad kommune har et sentralisert datasenter med fysiske servere og lagringsløsninger, som kjører VMWARE og vi har primært virtuelle løsninger i drift. Vi har i dag ca. 300 virtuelle servere i drift og flere løsninger i enten privat eller offentlig sky, vi kjører hybride-løsninger der det måtte være hensiktsmessig.

Vi har i dag nødstrømsløsning i form av UPS og aggregater som automatisk starter ved strømutfall, dette gjelder både våre datasentre og de fleste av våre helseinstitusjoner.

Andre løsninger vi har i drift som kan være av betydning

- Sentraliserte redundante brannmurer
- Egne brannmurer pr lokasjon og svitsjer som styres sentralt, med varsling, logging og egne sikkerhetspakker med virtuell patching av SD-enheter og kontrollere.
- MDM-system for sikring og utrulling av mobile enheter
- Standardisert på Android enheter, nettbrett og mobiltelefoner
- Microsoft Active Directory, ADSync og Entra ID.
- Komplette sikkerhetsløsninger fra Trend Micro.
- PRTG monitor for overvåking av nettverk, sensorer og servere m.m.
- IKT-tjenesten tar backup og har redundante løsninger på vårt serverrom.

## Arkitektur

Sikkerhetsarkitekturen til Harstad kommune følger disse prinsippene:

Nettet er delt inn i en rekke soner (eksempelvis DMZ, SD-nett til Drift og Utbygging, SD-nett til Bygg og eiendom, kamera, adgangskontroll, gjestenett, intern sone og sikker sone).

Det er et klart skille mellom tjenester og klienttyper inndelt i relevante sikkerhetspolicyer.

Tilgangen til tjenester reguleres gjennom bruk av sikkerhetsbarrierer (brannmurer, IPS, VLAN, pakkefilter, autentiseringsløsninger, VPN/SSL-GW, krav til klienter og tjenere osv.).

En sone har i utgangspunktet ikke tilgang til en annen sone med høyere sikkerhetsnivå, med mindre det er eksplisitt tillatt og regelregulert i en brannmur, da er det satt opp med spesifiserte porter og protokoller for slike åpninger.

En sone med høyere sikkerhetsnivå har ikke nødvendigvis tilgang til en sone med lavere sikkerhetsnivå.

Vi benytter ikke Internett på vår sikker sone, SD-nett, Kamera-nett, Adgangskontroll, eller andre sikre nett. Her må leverandør spesifisere åpninger og eller VPN-løsninger.

## Internsone

Harstad kommune har følgende tjenester lagt til intern sone: systemadministrative, fagnett, tekniske tjenester, administrative systemer, adgangskontroll, kamera, driftsnett, adm. av fjerntilgang, monitorering, samt servere som kan aksessere tjenestene i sikker sone.

## Sikkersoner

Våre tjenester og systemer som inneholder sensitive personopplysninger kjører i sikker sone. Her er det etablert en omfattende Citrix serverfarm til bruk for fagsystemene her. Serverne i sikker sone har også mulighet for tilgang til tjenester via Norsk Helsenett. Det er per i dag kun tilgang til NHN fra servernettet her.

## DMZ

Vi benytter DMZ for systemer som skal være åpne på Internett.

## Kravspesifikasjon i henhold til vår IKT-grunnmur

### Sentral infrastruktur:

Servere må kunne kjøres i et virtuelt Vmware-miljø med Windows server som operativsystem, om det ikke leveres sky-løsninger. Disse følger Microsoft sitt oppdateringsløp av programvare og operativsystem – og det samme må tilbudte løsninger kunne gjøre. Servere patches normalt sett i løp 2-3 dager etter de er sluppet. Alt av servere og klienter kjører Trend Vision One XDR.

For løsninger i sikker sone kjøres fagsystemene på Citrix – og tilbudte onprem løsninger må dermed kunne kjøre på eksisterende Citrix infrastruktur.

Løsninger som leveres skal benytte vårt eksisterende nettverk (LAN).

Nettverksstandarder

- 10/100/1000 BaseT nettverk
- Power over ethernet( 802.3af eller 802.3at)
- WIFI 802.11 g/n/ac
- Reservert og ikke registrert IP-adresse fra DHCP server
- Kryptering av all datakommunikasjon
- Kamera må støtte Milestone og kunne benyttes på denne løsningen.
- Adgangskontroll må støtte og kunne brukes fullt ut med Lenel OnGuard som Harstad kommune benytter som adgangskontroll-løsning.

Visma Enterprise HRM benyttes som kildesystem for de ansatte. HRM er integrert mot Microsoft Active Directory via Microsoft Identity Manager (MIM). Dermed opprettes, endres og stenges brukerkontoer i AD automatisk basert på kildedata fra HRM. Enhetsgrupper som kan brukes til tilgangsstyring bygges og vedlikeholdes automatisk basert på organisasjonsstrukturen. Brukere må kunne importeres fra Active Directory eller integreres for pålogging via AD-konto til den enkelte ansatte som har tilgang, vårt mål er ett passord for våre brukere. Tilgangen må gis via gruppestyring i Active directory.

Harstad kommune har som mål at nye system skal understøtte den etablerte infrastrukturen, slik at data i størst mulig grad registreres ett sted, og gjenbrukes i andre system. Det forventes at brukeradministrasjon av nye løsninger ikke er manuell, men håndteres via integrasjon mot eksisterende IAM løsning, enten MIM, AD eller Entra.

AD er også integrert mot Microsoft 365 via ADSync. Autentisering av skyløsninger skal dermed basere seg på integrasjon og autentisering via kommunens Entra ID. Dette for å ivareta identitet enkelt og sikkert. Autentisering mot Entra ID er sikret av et omfattende sett conditional access regler som blant annet er nedlåst til Norge og innrullerte enheter. Overvåking og sikring av skyløsninger kan dermed sikres både av Microsoft og Trend Micros sikkerhetstjenester. Tilbudte skyløsninger skal støtte dette.

Skyløsninger skal i leverandørens ende kunne sikres mot autentiseringsforsøk som kommer fra andre enn oppdragsgiver – spesielt hvis leveransen inkluderer sensitive data. Slike løsninger vil typisk gjøres tilgjengelig via Citrix i sikker sone, og skal da være nedlåst til kun å tillate trafikk fra våre avtalte IP adresser.

Alle nye løsninger, inkl SaaS, skal møte til enhver tid gjeldende sikkerhetskrav og basere seg på siste versjon av NSMs Grunnprinsipper for IKT sikkerhet.

## **Klientutstyr:**

Maskinparken for de ansatte er i hovedsak et Dell og Lenovo miljø av bærbare og stasjonære maskiner, som pt kjører Windows 10 og 11.

IKT benytter CapaInstaller og CapaOne til installasjon av OS og programvare, og klientprogramvare må kunne distribueres via denne løsningen. CapaOne ivaretar også oppdateringer av bios og drivere fortløpende. Maskinparken patches fortløpende via MS WSUS, og tilbudte løsninger må takle fortløpende oppdateringer av operativsystem og programvare.

Brukerne har ikke administrative rettigheter på pc'ene, og ethvert nytt system må kunne kjøre med standard brukerrettigheter på klientmaskinene.

## **Mobile enheter:**

Harstad kommune har standardisert på Android plattformen, og benytter mobiler og nettbrett fra Samsungs Galaxy serie. Apper som tilbys må dermed fungere på eksisterende plattform av mobile enheter.

For drift av mobile enheter benyttes Samsung Knox, slik at apper må kunne distribueres og, om nødvendig, prekonfigureres via denne MDM løsningen.

Anskaffelsen krever et nært samarbeid med IKT-avdelingen både under innføring og drift.

Passord og enkel dokumentasjon på hvordan man f.eks bytter ip-adresser på utstyr, må leveres til IKT-tjenesten, samt passord og eventuelt programvare for å utføre dette.

Løsninger som leveres skal helst automatisk motta oppdateringer fra leverandøren direkte, om oppdateringer må utføres av IKT-tjenesten, skal det leveres med dokumentasjon på hvordan dette skal gjennomføres, ellers må leverandør tilby å følge alle versjonsoppdateringer for løsningen.

Leverandører som skal ha tilgang til virtuell server og annen infrastruktur, må benytte seg av VPN-løsning fra Fortinet som IKT-tjenesten leverer, det må spesifiseres hvilket tilganger som trengs og eventuelt porter som må åpnes.

Zero Trust - det vil si at alt som ikke er spesifikt åpnet for, vil være stengt. Det er dermed et absolutt krav at leverandører i detalj spesifiserer sine løsninger. NSMs Grunnprinsipper for IKT Sikkerhet skal etterleves.

Tilbudte løsninger må understøtte eksisterende infrastruktur på en god og sikker måte. Løsninger som ikke kan tilpasses kommunens IKT arkitektur, vil ikke bli akseptert.