

Sikkerhetsplan

(SP)

Helse Midt-Norge

|  |  |
| --- | --- |
| Utarbeidet av: | Hallgeir NisjaBård GrødemKnut TorpDagfinn KrogJan HaugdalTore TetliauneGeir Reset Simonsen |
| **Godkjent:** |  |

Tabell - Dokumenthistorikk

|  |
| --- |
| **Dokumenthistorikk** |
| Versjon | Dato | Utført av | Endringsbeskrivelse |
| 0.9 | 2015-09-08 | Geir Reset Simonsen | Klar til intern revisjon |
| 0.971 | 2016-08-15 | Geir Reset Simonsen | Klargjort for ledermøte i HEMIT |
| 0.98 | 2016-09-19 | Geir Reset Simonsen | Klar for høring |
| 1.0 | 2016-11-10 | Geir Reset Simonsen | Godkjent |
| 1.1 | 2020-02-17 | Åsmund A. Nyre | Endringer i navn og koder for soner og søyler |
| 1.2 | 2020-02-07 | Åsmund A. Nyre | Feilretting – samsvar mellom versjonsnummer i EQS-dokument og vedlegg. Ingen innholdsendringer. |

Innholdsfortegnelse

[1 Innledning 5](#_Toc467575151)

[2 Klassifisering av system 12](#_Toc467575152)

[3 Ansvar 14](#_Toc467575153)

[4 Premissgivere 15](#_Toc467575154)

[5 Soner, Søyler og Celler 16](#_Toc467575155)

[6 Fysisk sikring 23](#_Toc467575156)

[7 Sikring av applikasjonstjenester 24](#_Toc467575157)

[8 Personellsikkerhet 27](#_Toc467575158)

[9 Databeskyttelse 28](#_Toc467575159)

[10 Katalogtjeneste 29](#_Toc467575160)

[11 Identitet og sertifikathåndtering 30](#_Toc467575161)

[12 Eksterne tjenester 32](#_Toc467575162)

[13 Konfigurasjonskontroll 33](#_Toc467575163)

[14 Infrastruktursikkerhet 34](#_Toc467575164)

[15 Sporbarhet og logghåndtering 36](#_Toc467575165)

[16 Systemvurderinger/godkjenninger 37](#_Toc467575166)

[17 Tjenestenivåer 38](#_Toc467575167)

Figur oversikt

[Figur 1 – Dokumenthierarki 7](#_Toc467575168)

[Figur 2 - Forhold til andre dokumenter og premissgivere 15](#_Toc467575169)

[Figur 3 - Soneinndeling 17](#_Toc467575170)

[Figur 4 - Søyler og celler i HMNs infrastruktur 20](#_Toc467575171)

[Figur 5 - Nettleser 24](#_Toc467575172)

[Figur 6- Web Service 24](https://prosjektweb.helse-midt.no/1280/Dokumenter%20fra%20gammel%20Prosjektweb/SP%20Dokumenter/990%20-%20Dokumenter%20til%20godkjenning/HMN%20Sikkerhetsplan.docx#_Toc467575173)

[Figur 7 - WS applikasjon 25](#_Toc467575174)

Tabell oversikt

[Tabell 1 - Dokumenthistorikk 2](#_Toc467575175)

[Tabell 2 - Definisjoner 10](#_Toc467575176)

[Tabell 3 - Søyler og beskrivelse av formål 19](#_Toc467575177)

[Tabell 4 - Sikkerhetskategorier for Infrastruktur 21](#_Toc467575178)

[Tabell 5 - Eksempler på bruksområder for sertifikater 31](#_Toc467575179)

# Innledning

Formålet med dette dokumentet er å etablere en Sikkerhetsplan (SP) for Helse Midt-Norge (HMN). SP skal bygge på HMNs styringsdokumenter for informasjonssikkerhet og ivareta kravene innenfor områdene:

* **Konfidensialitet**: *informasjon[[1]](#footnote-2)* må være sikret mot at uvedkommende får kjennskap til opplysningene
* **Integritet**: *informasjon* må være sikret mot utilsiktet eller uautorisert endring eller sletting og være korrekte, oppdaterte, relevante og tilstrekkelige som grunnlag for å yte helsehjelp
* **Tilgjengelighet**: *informasjon* som skal *behandles*, er tilgjengelig til den tid og på det sted det er behov for opplysningene
* **Sporbarhet** registrering av hendelser i et informasjonssystem, bl.a. med mål om å forebygge, avdekke og hindre gjentagelse av sikkerhetsbrudd.

SP er basert på følgende visjon:

 *Sikker tilgang til riktig informasjon, for riktig person,*

*til riktig tid, hvor som helst fra, med hva som helst.*

SP er forankret i HMN’s overordnede sikkerhetspolicy (se Figur 1 under) samt andre styringsdokumenter som omhandler informasjonssikkerhet. Den skal følges for all drift, (re)design og anskaffelser av IT-systemer, samt danne grunnlaget for avviksanalyser ved revisjoner.

SP bygger på prinsipper som tilfredsstiller nåværende og fremtidige brukerbehov. Den skal sørge for at IT-systemer har et rammeverk å forholde seg til ved endringer og nyimplementeringer. SP skal stille krav til sikker kommunikasjon mellom virksomheter og regioner, ved å spesifisere et rammeverk for autentisering og autorisasjon.

Det er utarbeidet retningslinjer som konkretiserer anvendelse av SP på forskjellige områder og gir eksempler på bruk. Retningslinjene gir konkrete føringer for hvordan SP kan realiseres i driften og hvordan IT-systemer skal implementeres i HMN.

SP består av følgende dokumenter:

* Dette dokumentet
* Presentasjon av Sikkerhetsplan (PowerPoint)
	+ Presentasjonen skal benyttes til å gi informasjon om og opplæring SPs innhold
* Handlingsplan til Sikkerhetsplan
Dokumentet beskriver nødvendige tiltak for at SP skal kunne realiseres fullt ut i HMN.
* Retningslinje 1 til SP – Sikkerhetsarkitektur
	+ Beskriver dagens sikkerhetsarkitektur/infrastruktur
* Retningslinje 2 til SP – Informasjonsflyt mellom soner
	+ Beskriver regler for informasjonsflyt mellom soner og celler i HMNs sikkerhetsarkitektur
* Retningslinje 3 til SP – Etablering og endring av tjenester
	+ Beskriver krav til IT-systemer som skal implementeres i HMNs infrastruktur
* Retningslinje 4 til SP – Passordpolitikk
	+ Beskriver HMNs passordpolitikk
* Retningslinje 5 til SP – Bruk av skytjenester
	+ Beskriver krav til løsninger som skal benytte seg av skytjenester
* Retningslinje 6 til SP – Herding av servere
	+ Beskriver krav til hvordan servere skal herdes
* Retningslinje 7 til SP – Herding av nettverkskomponenter
	+ Beskriver hvordan nettverkskomponenter skal herdes
* Retningslinje 8 til SP – Herding av klienter
	+ Beskriver hvordan klienter skal herdes
* Retningslinje 9 til SP – Delegeringsmodell for adminbrukere
	+ Beskriver delegeringsmodellen for gi administratorer tilganger

## Omfang og avgrensninger

Alle IT-systemer i HMN som produserer, lagrer, transporterer eller på annen måte behandler informasjon elektronisk er underlagt SP. Dette gjelder også test og utviklingsmiljøer.

Alle brukere av IT-systemer er også underlagt SP.

For å unngå unødige revisjoner av SP skal det som hovedregel brukes henvisninger til andre styringsdokumenter som for eksempel:

* Lover og forskrifter
* Norm for informasjonssikkerhet i helsesektoren med faktaark og veiledere (Normen)
* Overordnet sikkerhetspolicy for HMN

Figur 1 under viser en oversikt over aktuelle styringsdokumenter.



Figur 1 – Dokumenthierarki

Bare unntaksvis skal utdrag fra dokumenter det henvises til gjengis og bare dersom det er helt nødvendig for forståelsen av innholdet.

### Ansvar og revisjon av Sikkerhetsplanen

Dokumentstrukturen legger til rette for en enklere revisjonsprosess knyttet til enkelte deldokument i Sikkerhetsplanens retningslinjer og vedlegg. Følgende tabell viser ansvar og revisjonssyklus. Alle dokumentene er lagt inn i kvalitetssystemet EQS og revisjon og varsling følges opp i henhold til rutiner i dette.

|  |  |  |
| --- | --- | --- |
| Dokument | Ansvar | Revisjon |
| HMN Sikkerhetsplan (hoveddokument) | Hemit - Arkitektur | Hvert 2. år |
| Retningslinje 1 - Sikkerhetsarkitektur | Hemit - Arkitektur | Hver 3. mnd |
| Retningslinje 2 – Informasjonsflyt mellom soner | Hemit - Arkitektur | Årlig |
| Retningslinje 3 – Etablering og endring av tjenester | Hemit - Arkitektur | Årlig |
| Vedlegg A – Detaljdesign dokumentasjon |  | Hver 3. mnd |
| Vedlegg B – Mal for innhenting av informasjon om skytjenesten | Hemit - Arkitektur | Hver 3. mnd |
| Vedlegg C – Flytdiagram | Hemit - Arkitektur | Årlig |
| Vedlegg D – Kravhjul IT-system | Hemit - Arkitektur | Årlig |
| Vedlegg E – Kravhjul IT Infrastruktur | Hemit - Arkitektur | Årlig |
| Retningslinje 4 – Passordpolitikk | Hemit - Arkitektur | Hvert 2. år |
| Retningslinje 5 – Bruk av skytjenester | Hemit - Arkitektur | Årlig |
| Retningslinje 6 – Herding av servere | Hemit – Serverdrift | Hver 3. mnd |
| Retningslinje 7 – Herding av nettverkskomponenter | Hemit – Nettverksdrift | Hver 3. mnd |
| Retningslinje 8 – Herding av klienter | Hemit – Klientdrift | Hver 3. mnd |
| Retningslinje 9 – Delegeringsmodell for admin brukere | Hemit - Arkitektur | Hver 3. mnd |

## Målgruppe

Målgruppen for SP er sikkerhetsansvarlige, beslutningstagere, IT-sjefer, prosjekter og prosjektledere, alle avdelinger i Hemit og andre som har befatning med IT-systemer (applikasjoner, infrastruktur med mer) i HMN.

Ved tilsyn vil SP, sammen med Normen, benyttes som målepunkt/premissgivere.

## Avvik

Det skal søkes godkjenning for alle IT-systemer som avviker fra de krav og føringer som Sikkerhetsplan med underliggende dokumenter gir. Alle avvik skal behandles av Hemit IT Sikkehetsforum (HITS), som er nedsatt av ledelsen i Hemit og ledes av rollen sikkerhetsrådgiver.

Avvik som ikke avklares i HITS eller er av et slikt omfang at større prinsipielle beslutninger må tas, løftes av sikkerhetsrådgiver til Regionalt Informasjonssikkerhets Forum (RIF) for behandling.

HITS og RIF gir anbefalinger til virksomhetens leder hvor det er avdekket eventuell mangel på oppfyllelse av lov-, norm eller informasjonssikkerhetsprinsippkrav. Før produksjonssettelse, skal virksomhetens leder vurdere om det er mulig å iverksette tiltak i virksomheten slik at leveransen kan godkjennes, og ut fra dette godkjenne eller avvise leveransen.

Alle sikkerhetsavvik som er behandlet i HITS og RIF skal fravikshåndteres i tråd med EQS prosedyre **«**Fravikstillatelse, prosedyre for forespørsel og behandling» ([ID:2083](http://eqshemit.helsemn.no/index.pl?pid=hemit&DocumentID=2083))

## Sammendrag

Bruken av IT i spesialisthelsetjenesten endrer seg raskt og flere kritiske funksjoner i pasientbehandlingen baseres på IT. Helseforetakene ønsker en desentralisert behandling og oppfølging av pasienter og det krever at **IT-systemene** **åpner opp for at spesialister innenfor fagområder kan bidra i pasientbehandling uten fysisk tilstedeværelse**.

I tillegg krever samhandlingsreformen og andre politiske føringer en mer effektiv samhandling mellom de forskjellige ledd i helsetjenesten. IT blir et svært viktig og avgjørende verktøy for å effektivisere samhandlingen.

Dette krever at SP er fleksibel og gir føringer for nye behov som oppstår som en følge av endringer i rammebetingelser. Tilpasningen må skje takt med behovene til pasient og behandler og i tråd med kravene fra ledelsen. Samtidig som personvernet og pasientsikkerheten ivaretas i henhold til lovkrav, Normen, veiledere og Datatilsynet. Alle krav skal ivaretas uansett om data er i bruk (behandling), under oppbevaring (lagring) eller under transport (datakommunikasjon).

Et viktig utgangspunkt for en sikker behandling av data er en entydig identifisering av brukerne (autentisering). IT-systemene skal autentisere brukerne entydig og deretter gi de nødvendige tilganger (autorisasjon) til data som behandles. Personlige sertifikater og tilhørende nøkkelpar skal benyttes for å identifisere brukere på en entydig og sikker måte.

Brukernes autorisasjon skal tildeles til riktig tid og fortløpende endres i henhold til arbeidsforhold (rolle).

Mobilitet blir viktigere og viktigere i forhold til å implementere en mer effektiv pasientbehandling. Mobilitet krever en fleksibel infrastruktur som gir brukere tilgang til den informasjonen de trenger og er autorisert for, der de til enhver tid befinner seg.

Klienten (brukerens IT utstyr) må sikres. Bruk av mobile klienter øker i omfang og skjerper kravene til sikring av data som behandles på dem. Kravet er at data ikke lagres lokalt på klientene uten at de krypteres for åforhindre at sensitiv informasjon kommer på avveie ved eventuelt tap. Videre må det sikres at klienter ikke bringer ondsinnet kode inn i virksomhetens IT-systemer.

Sikre klienter er viktig for sikker databehandling, men minst like viktig er en sentral infrastruktur med sikkerhetsbarrierer og andre sikkerhetsmekanismer som oppdateres i tråd med trusselbildet. Det er et overordnet mål å implementere en fleksibel, enkel og dermed sikker brannmur og nettverkstopologi.

Det er viktig med enhetlige administrasjons- og vedlikeholdstjenester for alle sikkerhetssystemer.Deriblant løsninger som sikrer at logger oppbevares og sikres i henhold til lovgiving for slik oppbevaring og sikring, samt at det finnes systemer og rutiner for å analysere og rapportere fra sikkerhetslogger.

## Definisjoner

Tabell - Definisjoner

|  |  |
| --- | --- |
| Term | Forklaring |
| Brannmur | Maskinvare og/eller programvare som beskytter datanettverk mot uønsket kommunikasjon. |
| BYOD | Bring Your Own Device. Enheter som brukerne selv bringer med seg for eksempel nettbrett, telefoner, etc. |
| Cloud computing | Se Skytjenester |
| Databehandlingsansvarlig | Den som bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes, hvis ikke databehandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven, jf. helseregisterloven § 2 e), pasientjournalloven § 2 e) og personopplysningsloven § 2 nr. 4) (her benyttes begrepet ”behandlingsansvarlig”). Det presiseres at det er virksomheten som er databehandlingsansvarlig for behandling av helse- og personopplysninger. Ansvaret skal ivaretas av den daglige ledelsen av virksomheten, og virksomheten er pliktsubjekt. |
| MU | Elektromedisinsk Utstyr (MU) ny benevnelse for Medisinteknisk utstyr (MTU)jfr Forskrift om håndtering av medisinsk utstyr § 4 |
| Federering | Federering benyttes for å gi brukere fra to forskjellige virksomheter tilgang til virksomhetenes IT-systemer uten at man må duplisere begge virksomhetenes brukeridentiteter. Det etableres en tillit (trust) mellom de to virksomhetene hvorpå foretak A utsteder et signert token (claim) når en bruker i foretaket ønsker tilgang til en ressurs fra foretak B. Foretak B evaluerer tokenet og gir brukere tilgang basert på dette.   <http://en.wikipedia.org/wiki/Federated_identity> |
| IDP | Identitetstilbyder (Identity Provider) |
| IDS | Intrusion Detection System er løsninger som settes passivt inn i et nettverk for å detektere angrep og avvik fra normal datakommunikasjon. |
| Normen | Norm for informasjonssikkerhet i helsesektoren, <http://www.normen.no/>  |
| Klienter | Alle typer av brukerutstyr (ikke servere) som kobles til nettverksinfrastrukturen. |
| MTU | Se MU. |
| Perimeter | Ytre grense for et nettverk. |
| Proxytjeneste | En proxytjener, proxyserver eller mellomtjener er en server som står mellom en klient og en annen server. Ofte er en proxytjener satt opp for å begrense tilgangen til enkelte websider fra et nettverk. |
| Skytjenester | Nettskyen (eng: cloud computing) er en betegnelse for alt fra dataprosessering og datalagring til programvare på [servere](http://no.wikipedia.org/wiki/Tjener) som står i serverparker tilknyttet [internett](http://no.wikipedia.org/wiki/Internett) administrert av skyleverandører |
| Sone | Avhengig av informasjonen som skal behandles (Informasjonsklasse) plasseres en tjeneste i en sone. |
| Celle | Kombinasjonen av Sone og Tjenestesøyle angir i hvilken Celle en tjeneste skal produseres. |
| Tjenestesøyle | En kategorisering av tjenester som skal produseres. Plassering i søyler gjøres med bakgrunn i type tjeneste/løsning. |
| Transparente nettverk | HMNs nettverksdesign muliggjør at nettverk kan tilbys med forskjellige typer teknologier der det måtte være behov, med et enhetlig sikkerhetsnivå. |
| Virksomhetsleder | Den som er ansvarlig for helsehjelpen som ytes og informasjonssikkerheten i den enkelte virksomhet. |
| VPN | Virtuelle Private Nettverk: virtuelt privat datanettverk, er betegnelsen på en datateknikk som anvendes for å skape «punkt-til-punkt»-forbindelser, såkalte «tunneler», gjennom et annet datanett (som f.eks. internett). Et VPN kan være både kryptert og ukryptert. |
| WAN | Wide Area Network (WAN) er et datanettverk som dekker et stort geografisk område. Det beste eksempelet på et WAN er Internett. |
| WS-Security | Er en utvidelse av protokollen for utveksling av XML-baserte meldinger i datanettverk, SOAP. Utvidelsen implementerer sikkerhet i XML-baserte meldinger som utveksles av WEB tjenester.Is an extension to [SOAP](https://msdn.microsoft.com/en-us/library/ms995800.aspx) to apply security to [Web services](https://msdn.microsoft.com/en-us/library/ms972326.aspx). It is a member of the [Web service specifications](https://msdn.microsoft.com/en-us/library/ms951274.aspx) and was published by [OASIS](https://www.oasis-open.org/) |
| WS-I Basic Security | Det er en åpen sikkerhetsprofil som validerer transportsikkerhet, sikkerheten i SOAP meldingen og andre sikkerhetsbetraktninger.Is an interoperability profile that addresses transport security, SOAP messaging security, and other security considerations. |
| Sikkerhetsbarriere | En sikkerhetsbarriere kontrollerer informasjonsflyten mellom sonene slik at kun eksplisitt tillatt nettverkstrafikk flyter igjennom den. |
| IPS | Intrusion Prevention System (IPS) er en sikkerhetstjeneste som overvåker flyten i nettverkstrafikk og forsøker å oppdage og forhindre utnyttelse av sårbarheter. |
| IDP | Identity Provider (IDP) er ansvarlig for å forsyne brukere med identiteter som kan benyttes til å autentisere seg i et IT system |
| Proxy tjeneste | En applikasjonstjeneste som utgir seg for å ha samme egenskaper som en annen applikasjonstjeneste. |
| CA | Certificate Authority (CA) er en tjeneste som utsteder elektroniske sertifikater |
| Karantenenettverk | Et nettverk med et svært begrenset tjenesteutvalg som IT utstyr blir tvunget inn i når utstyret ikke er kompatibelt med sikkerhetskravene. |

# Klassifisering av system

Alle IT-systemer som benyttes i HMNs infrastruktur må klassifiseres i forhold til hvilken informasjon de behandler. IT-systemer klassifiseres i forhold til informasjonssensitivitet og i henhold til kritikalitet.

Informasjonssensitivitet har fem nivåer:

* **Informasjonsklasse 1** – Helseopplysninger
Dette er pr. definisjon i Normen det samme som Sensitive Personopplysninger (jfr Personopplysningsloven)
* **Informasjonsklasse 2** – Bedriftsinterne
Ikke-sensitive personopplysninger eller andre opplysninger i virksomheten som ikke skal eksponeres eksternt
* **Informasjonsklasse 3** – Indirekte identifiserbare helseopplysninger
Med avidentifiserte («indirekte identifiserbare helseopplysninger») menes i Normen helse- og personopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson, og hvor identitet bare kan tilbakeføres ved sammenstilling med de samme opplysninger som tidligere ble fjernet (jf. helseregisterloven § 2 b). For å regnes som indirekte identifiserbare helseopplysninger, skal dataene være bearbeidet slik at de uten løpenummer fremstår som anonyme. (Kan spores tilbake.)
* **Informasjonsklasse 4** – Anonymiserte data
Med «anonymisert» menes i Normen helse- og personopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson (jf. helseregisterloven § 2 nr 3.. (Kan ikke reverseres / spores tilbake.)
* **Informasjonsklasse 5** – Åpne data
Alle andre typer data, som kan eksponeres utenfor virksomheten.

Gradering i henhold til Beskyttelsesinstruksen (<https://lovdata.no/dokument/INS/forskrift/1972-03-17-3352>) er informasjonsklasse 2.

Gradering i henhold til Sikkerhetsloven (<https://lovdata.no/dokument/NL/lov/1998-03-20-10>) dekkes ikke i dette dokument.

I forhold til kritikalitet skal dette vurderes i henhold til Normens [Faktaark 4](https://ehelse.no/Documents/Normen/Faktaark%2004%20-%20Kartlegge%20og%20klassifisere%20systemer.pdf), “Kartlegging og klassifisering av systemer i henhold til kritikalitet i forhold til behov for tilgjengelighet”. For å klassifisere et IT-system skal metodikken i [Faktaark 5](https://ehelse.no/faktaark-05-fastsette-niva-for-akseptabel-risiko) «Fastsette akseptkriterier for tilgjengelighet, konfidensialitet, integritet» benyttes.

Følgende prioriteter er definert i Faktaark 4:

* **Prioritet 1**: IT-systemer hvor stopp av tjeneste er eller kan være livstruende for pasient inklusive feilbehandling av pasient, eller kritisk for virksomhetens drift
* **Prioritet 2**: IT-systemer hvor stopp av tjeneste kan få alvorlige konsekvenser, f.eks. medføre
	+ - betydelig merarbeid for personell
	+ - tapt effektivitet i virksomheten
* **Prioritet 3**: IT-systemer hvor stopp av tjeneste kan føre til svekkelse av pasientens tillit
* **Prioritet 4**: IT-systemer hvor stopp inntil 72 timer kan aksepteres
* **Prioritet 5**: IT-systemer som ikke er prioritert

Det er virksomhetsleder som har ansvar for å kartlegge og klassifisere alle IT-systemer som behandler helse- og personopplysninger i virksomheten. I praksis er oppgavene knyttet til dette delegert til avdelingsledere / systemeiere.

# Ansvar

Ansvarsfordeling er i henhold til Norm for Informasjonssikkerhet, [Faktaark 1](https://ehelse.no/faktaark-01-ansvar-og-organisering).

# Premissgivere

Figur 2 nedenfor beskriver hvordan SP forholder seg til andre, relevante dokumenter.



Figur - Forhold til andre dokumenter og premissgivere

Overordnet for sikkerhet i HMN er Nasjonale føringer som lover og forskrifter, med tilhørende Norm for informasjonssikkerhet i helsesektoren (inklusive faktaark).

Videre har HMN en Regional Sikkerhetspolicy som støtter opp under de nasjonale føringer.

SP er underlagt alle føringer og dokumenter nevnt overfor og skal beskrive hvordan disse skal implementeres i HMNs arkitektur. Underliggende dokumenter for SP er planer og veiledninger/instrukser.

Teknologistrategien beskriver de teknologiske føringer som gjelder for sikkerhetstjenester og løsninger i HMN.

# Soner, Søyler og Celler

For å kunne realisere Sikkerhetsplanen sin visjon skal en felles enhetlig infrastruktur ligge til grunn. Visjonen legger opp til at informasjon i alle informasjonsklasser behandles på en fleksibel, robust og sikker måte over samme infrastruktur.

For å kunne lagre, behandle og transportere informasjon i forskjellige informasjonsklasser på en sikker måte, **defineres soner**. Sonene bidrar til at informasjon behandles i tråd med kravene som stilles til dennes informasjonsklasse.

HMN benytter tjenestesøyler og celler for å realisere visjonen med at hvem som helst, som er autentisert og autorisert, hvor som helst fra, og med bruk av alle typer klienter, kan koble seg til en vilkårlig ressurs, sikkert, stabilt og sømløst. Tjenestesøyler og celler er definert for at all infrastruktur og alle IT-systemer som behandler samme type informasjon underlegges like krav og sikkerhetsmekanismer.

Dette kapitlet inneholder generelle definisjoner og krav. Inklusive overordnede tekniske krav til infrastrukturen som skal ligge til grunn for å realisere tjenestesøyler og celler. De krav som stilles til IT-systemer som skal inn i de definerte celler beskrives også her.

## Soner

HMN har opprettet fem administrativt kontrollerte soner: **sikker sone, intern sone, åpen sone, DMZ og servicesone** (se Figur 3 nedenfor). I tillegg benyttes **eksterne soner**, somHMN ikke har administrativ kontroll over. Mange IT-systemer vil være avhengig av å kommunisere med IT-systemer i eksterne soner.

IT-systemer og utstyr skal tilordnes soner i tråd med hvilken informasjonsklasse informasjonen de behandler tilhører, hvilken informasjon som skal utveksles mellom soner og i hvilke retning informasjonsflyten skal gå.

Sikkerhetsbarrierer skal kontrollere informasjonsflyten mellom sonene slik at kun eksplisitt tillatt nettverkstrafikk traverserer fra utsiden og inn til de forskjellige sonene. Det skal minimum eksistere én sikkerhetsbarriere mellom hver sone. Dette gir kontroll over tilgangen til informasjon i de forskjellige informasjonsklassene.

Informasjonsflyten mellom flere forekomster av like soner skal i enkelte tilfeller kontrolleres av sikkerhetsbarrierer hvis de er opprettet med formålet å separere informasjon (for eksempel på grunn av tjenstlige behov eller juridiske føringer).

Retning på informasjonsflyten skal ta utgangspunkt i at det ikke skal kunne initieres informasjonsflyt fra en sone lengre ut og inn mot en sone lengre inn (se Figur 3 - Soneinndeling) uten at særskilte sikkerhetstiltak er iverksatt.

Tabell : Soner med navn og kode

|  |  |  |
| --- | --- | --- |
| Sone | Navn | Kode |
| Sikker sone | Secure | S |
| Intern sone | Internal | I |
| Åpen sone | Open | O |
| Service-sone | Service | C |
| DMZ sone | DMZ | Z |
| Ekstern sone | External | E |



Figur - Soneinndeling

### Sikker sone

Sikre soner tilordnes IT-systemer og utstyr som behandler sensitive personopplysninger[[2]](#footnote-3) som er klassifisert i informasjonsklasse 1 (helseopplysninger) og 3 (avidentifiserte helseopplysninger). Disse sonene tilordnes IT-systemer og utstyr som har høyeste sikkerhetsklarering i HMN.

Det skal eksistere sikre soner for grupper av IT-systemer som behandler sensitive personopplysninger.

IT-systemer og utstyr som er tilordnet en sikker sone kan etablere informasjonsflyt med nødvendige IT-systemer i andre soner.

### Intern sone

Intern sone tilordnes IT-systemer og utstyr som lagrer eller behandler bedriftsintern og anonymisert informasjon som er klassifisert i informasjonsklasse 2 (bedriftsintern) og 4 (anonymisert).

IT-systemer og utstyr som er tilordnet intern sone kan ikke etablere informasjonsflyt med IT-systemer i sikker sone uten at særskilte sikkerhetstiltak gjennomføres.

### Åpen sone

Åpen sone tilordnes IT-systemer og utstyr som lagrer eller behandler informasjon som er offentlig tilgjengelig og er klassifisert i informasjonsklasse 5 (åpne).

IT-systemer og utstyr som er tilordnet åpen sone kan ikke etablere informasjonsflyt med IT-systemer i sikker eller intern sone uten at særskilte sikkerhetstiltak gjennomføres.

Det settes ingen begrensninger til utstyr som tilknyttes nettverkspunkter som er tilordnet åpen sone. De vil ikke være beskyttet av fysisk sikring i form av adgangskontroll.

### Service Sone

Sikkerhetsrelaterte IT-systemer og utstyr tilordnes service sone som skal sikre informasjonsflyt som etableres mellom flere soner.

Det skal ikke lagres informasjon i denne sonen.

### DMZ

En DMZ eller demilitarisert sone tilgjengeliggjør HMNs offentlige tjenester mot eksterne nettverk.

### Ekstern sone

Ekstern sone tilordnes IT-systemer og utstyr som HMN ikke har administrativ kontroll over. Eksempler er Norsk Helsenett og Internett.

## Søyler og celler

Søyler definerer logisk nettverk som har spesifikke formål (se Figur 4). De logiske nettverkene grupperer IT tjenester som har samme formål.

Celler er krysningspunktet mellom soner og søyler. Hver enkelt celle definerer kravene til sikkerhetsegenskaper IT-systemer må tilfredsstille og hvilke sikkerhetsbarrierer som må være på plass.

Tradisjonelt sett likestilles sikkerhetsbarrierer med brannmurer. Sikkerhetsbarrierer i HMNs modell vil i tillegg være løsninger som flytter sikkerhetsbarrierene ut på klienten eller bygges inn i applikasjonene.

Figur 4 nedenfor viser en oversikt over definerte søyler. Søylene har ulike formål og de stiller individuelle sikkerhetskrav til IT-systemer, utstyr som kobles til, brukerkategorier.

Tabell - Søyler med navn, kode og beskrivelse av formål

|  |  |  |  |
| --- | --- | --- | --- |
| **Søyle** | **Navn** | **Kode** | **Formål** |
| Intern tjenestesøyle  | Internal | I | Denne søylen skal inneholde IT tjenester som tilfredsstiller krav som stilles til tjenester i HMNs datasenter[[3]](#footnote-4) |
| Ekstern tjenestesøyle | External | E | Denne søylen skal inneholde IT tjenester tilsvarende Intern Tjenesøyle, men gjøres tilgjengelig fra en ekstern tjenestetilbyder, for eksempel en skytjeneste |
| Lokal tjenestesøyle | Local | L | Denne søylen skal inneholde IT tjenester som er lokalisert på lokale datarom i HMN |
| Klientsøyle | Client | C | Denne søylen skal inneholde alle typer klienter (PCer, mobile enheter, IP-telefoner og så videre). Klienter som tilhører gruppen BYOD tilhører også denne søylen |
| MTU/TU-søyle | Technical devices | T | Denne søylen skal inneholde medisin teknisk utstyr og annet teknisk utstyr, som ikke tilfredsstiller sikkerhetskravene som stilles til klient eller tjenestesøyler |
| Management søyle | Management services | MS\* | Denne søylen skal inneholde drifts- og overvåkingstjenester. For eksempel er sikkerhetskopieringstjenesten plassert her |
| Administrasjons søyle | Administration | A | Denne søylen skal inneholde utstyr som produserer tjenester for administratorer av IT tjenester. |
| Katalogtjeneste søyle | Directory services | DS\* | Denne søylen skal inneholde felles katalogtjenesten(e) som benyttes i HMN |

\*) Disse tjenesteområdene er felles for flere soner derfor benyttes det to tegn for søyle-koden og ingen kode for sone.



Figur 4 - Navn og koder for nettverkssoner og tjenesteområder I HMNs infrastruktur

De ulike cellene skal ha dedikerte sikkerhetsegenskaper og det skal stilles eksplisitte sikkerhetskrav til IT-systemene som skal tilordnes dem.

Retningslinje 1 til SP – «Sikkerhetsarkitektur» angir cellenes sikkerhetsegenskaper og Retningslinje 3 til SP «Etablering og endring av tjenester» definerer sikkerhetskravene som stilles til IT-systemer som tilordnes de ulike cellene.

### Krav og sikkerhetsegenskaper til IT infrastruktur

For at man skal få benyttet konseptet med soner, søyler og celler stilles det krav til den underliggende infrastrukturen og de løsninger som skal benytte infrastrukturen.

De sikkerhetsegenskaper som underliggende infrastruktur og løsninger må støtte er listet i Tabell 4 under.

Tabell - Sikkerhetskategorier for Infrastruktur

|  |  |
| --- | --- |
| Sikkerhetskategorier | Egenskap/beskrivelse |
| S1 | Nettverksikkerhet (kommunikasjon, kryptering, trådløssikkerhet, Høytilgjengelighet) | Integritetsbeskyttelse av nettverksinfrastrukturen, inkludert brannmurer, IPS-løsninger og forhindring av datatap. Kryptering av data under overføringAutentisering og kryptering av trådløse endepunkt. Krav som understøtter høytilgjengelighet i infrastrukturen.Aksess kontroll og autentisering av brukere og endepunkter (trådbaserte og trådløse arbeidsstasjoner, MTU osv). |
| S2 | Antivirus, patch managment, herding og konfigurasjonskontroll | Bruk av antivirusprogramvare og prosesser/prosedyrer for patch management. Inklusive herding av infrastrukturkomponenter. |
| S3 | Fjernaksess | Sikker fjerntilgang, over internett eller privat WAN. |
| S4 | Logging, sporing og monitorering | Krav som stilles til at infrastruktur benytte tjenester som logger, sporer og overvåker. |
| S5 | Endepunkt | Krav som stilles til endepunkter i infrastrukturen (servere, klienter) |
| S6 | Brukerautentisering, autorisasjon og terminering | Autentisering og autorisasjon for administrasjon av infrastrukturkomponenter. |

For å realisere kravene som stilles til cellenes sikkerhetsegenskaper skal underliggende infrastruktur og IT-systemer etableres med utgangspunkt i gitte standard teknologier. De valgte teknologiene er nærmere beskrevet i Retningslinje 1 – «Sikkerhetsarkitektur».

### Krav til sikkerhet i IT-systemer

Avhengig av hvilken celle et IT-system tilordnes, stilles det forskjellige sikkerhetskrav. Sikkerhetskravene grupperes i følgende kategorier:

1. Systemkontroll
2. Kontinuitet
3. Autentisering og Autorisasjon
4. Tilganger til/fra andre celler/tjenester
5. Dokumentasjon
6. Organisasjon

Retningslinje 3 til SP – «Etablering og endring av tjenester», definerer de sikkerhetskrav som stilles til IT-systemer avhengig av hvilken celle de tilordnes.

## Perimeternettverk

Dagens sikkerhetsarkitektur baserer seg på sikkerhetsmekanismen brannmur i rollen foretaksbarrierer for å sikre perimeternettverket. Tjenestebarrierer (brannmurer) etablert for å ivareta sikkerheten i de IT-systemene som danner grunnlaget for de IT tjenestene som tilbys.

Fremover skal foretaksbarrierene fortsatt være en del av sikkerhetsarkitekturen, men hovedoppgavene vil i hovedsak bli:

* Å beskytte mot mulige «Denial of Service angrep» mot serverressurser og IT-systemer i infrastrukturen, samt begrense konsekvensene av eventuelle «broadcast stormer» som påvirker tilgjengeligheten til vitale IT tjenester
* Å beskytte mot at ormer spres fra en celle til et annen. Beskyttelsesmekanismen skal holdes oppdatert slik at løsningen også beskytter mot nye varianter
* Å bidra til en hensiktsmessig trafikkflyt i nettverket

# Fysisk sikring

Fysisk sikring skal definere kravene til adgangskontroll for ulike fysiske områder og fysisk tilgang til IT utstyr. I tillegg skal det defineres hvordan de forskjellige fysiske områder skal sikres mot for eksempel brann- og vannskader. Fysisk sikring skal følge [Faktaark 17 - Fysisk sikring av områder og utstyr](https://ehelse.no/faktaark-17-fysisk-sikring-av-omrader-og-utstyr).

For HMN er det utarbeidet en kravspesifikasjon for datarom som skal følges. Denne ligger i [EQS](http://eqshemit/cgi-bin/document.pl?pid=hemit&DocumentID=1834).

# Sikring av applikasjonstjenester

I mange sammenhenger skal HMN tilby applikasjonstjenester til eksterne konsumenter. Eksempler på dette er tjenester som innbyggerne skal ha tilgang til via Digitale innbyggertjenester. Applikasjonstjenestene skal være i implementert som beskrevet i tiltak 12: ‘Tjenesteorientert arkitektur i spesialisthelsetjenesten’ kap.9 utarbeidet av NIKT.

Retningslinje 1 til SP – «Sikkerhetsarkitektur» beskriver hvordan disse applikasjonstjenestene skal nås fra eksterne konsumenter og sikres på nettverkslaget.

Sikring av applikasjonstjenesten i de overliggende lagene skal implementeres i tråd med følgende arkitektur:

1. Konsumenten skal autentisere seg i forhold til en Identitetstilbyder (IDP) som applikasjonstjenesten stoler på
2. En applikasjonsbrannmur mellom konsumenten og applikasjonstjenesten skal utføre kontroll med at konsumenten er autentisert og at trafikkflyten mellom dem ikke inneholder ondsinnet kode
3. Tjenestebussen (ESB) vil tilby en proxytjeneste for applikasjonstjenester som ikke håndterer standardiserte sikkerhetstoken
4. Applikasjonstjenesten skal hente brukeridentifikasjon fra et sikkerhetstoken, autorisere brukeren og gi rettmessig tilgang til informasjonen applikasjonstjenesten behandler



Figur - Nettleser

Figur - Web Service

 

Figur - WS applikasjon

Applikasjonstjenesten skal kunne forutsette at aktiv bruker er tilstrekkelig sikkert autentisert før konsumenten når applikasjonstjenesten, slik at både bruker ID, autentiseringsstyrke og eventuelt andre opplysninger er tilgjengelig for tjenesten i et standardisert og verifisert sikkerhetstoken formidlet av applikasjonsbrannmuren.

Applikasjonstjenesten skal behandle informasjon på vegne av bruker. Den skal ha rettigheter som en privilegert system- eller tjeneste-bruker som kan behandle informasjon på vegne av alle brukere. Applikasjonstjenester skal autorisere brukere tilstrekkelig til å gi de rettmessig tilgang til informasjon.

Applikasjonstjenester skal kun benyttes av brukere som er definert i IDP-er som kan autentisere brukere med det autentiseringsnivået den krever. Det skal inngås gjensidige avtaler med IDP-er som autentiserer brukere, for å sikre tilstrekkelig kvalitet på administrasjon og forvaltning av brukere eller autentisere brukerne i eget sikkerhetsregime (egen IDP).

Sikkerhetsfunksjonene i applikasjonsbrannmuren skal sørge for:

* at brukere blir autentisert i brukerens tilhørende IDP
* å formidle et validert SAML token til applikasjonstjenesten
* å inspisere trafikkflyten mellom konsument og applikasjonstjeneste for å fjerne ondsinnet kode
* å rute trafikkflyten til enten proxy tjeneste på ESB eller applikasjonstjenesten, avhengig av applikasjonens funksjonalitet

Brukerinformasjonen skal foreligge i et gyldig og signert token.

En generisk proxy tjeneste på tjenestebussen skal pakke ut og videreformidle bruker og eventuelt tilhørende informasjon fra SAML token til applikasjonstjenester som ikke håndterer det selv.

For å understøtte Single Sign On for applikasjonstjenester kreves det at PC/Nettverks pålogging minimum har den autentiseringsstyrke applikasjonstjenestene krever. Hvis autentiseringsstyrken er tilfredsstillende, skal sikkerhetstoken fra påloggingen gjøres tilgjengelig for applikasjonstjenesten som kan autorisere brukeren uten ny pålogging. I motsatt fall skal applikasjonstjenesten kreve ny pålogging som tilfredsstiller kravet applikasjonstjenestens stiller til autentiseringsstyrke.

I en tjenesteorientert arkitektur der tjenestene skal kunne benyttes både direkte og inngå i en prosessflyt, stilles det nye krav til autentiseringsløsninger mellom konsument og tilbyder. For å håndtere ende-til-endekryptering, autentisering og sporbarhet, skal informasjonssikkerhetsmekanismene rundt tjenestene baseres på WS-Security og WS-I Basic Security profiler. Tjenestebussen skal tilby funksjonalitet for håndteringen av WS-Security for å forenkle håndteringen av informasjonssikkerheten for tjeneste- konsument og tjenestetilbyder.

Web baserte løsninger må kunne håndtere et standardisert token og plukke ut nødvendig informasjon for å autorisere brukeren.

Det stilles samme krav til logging og sporing når en tilgjengelig gjør sensitive personopplysninger via applikasjonstjenester, som tilgang via personlig autentisering til disse applikasjonene.

En tjenestebasert arkitekturmodell legger til rette for rollebasert autentisering. Det bygges opp en rollemodell som defineres i tilgangssystemet og beskriver hvilke operasjoner de forskjellige rollene skal kunne utføre. Roller kobles mot brukere eller brukergrupper i tilgangssystemet. Verifikasjon av tilgang til applikasjonstjenester, og funksjoner i applikasjonene kan gjøres mot tilgangssystemet, men vil i overskuelig fremtid være avhengig av det enkelte system sin rollemodell og tilgangsstyring.

# Personellsikkerhet

Alle som utfører tjeneste i virksomheten skal underskrive databrukerkontrakt (taushetserklæring).

Det skal så langt som mulig sikres gjennom tilgangsstyring at ingen brukere skal ha tilgang til annen informasjon enn det de har tjenstlige behov for.

I tillegg skal alle brukere som skal ha tilgang til data i informasjonsklasse 1 og 2 ha separat opplæring i informasjonssikkerhet.

## Opplæring

Ved ansettelse skal alle ansatte bli orientert om og forelagt Brukerinstruks. Hver enkelt ansatt skal signere på at Brukerinstruks er gjennomgått og forstått.

Alle ansatte forpliktes også til å gjennomføre pålagt e-læring og delta på holdningsskapende sikkerhetskampanjer, det skal signeres på at disse er gjennomgått.

# Databeskyttelse

Med databeskyttelse menes sikring av data når de overføres mellom to celler (transport), samt sikring av tilgang til dataene i en celle (lagring).

Sikring av data i en celle skal gjøres sentralt, men data skal kun lagres lokalt når dette er nødvendig ut fra et tjenstlig behov og skal da alltid lagres kryptert.

Håndtering av lagringsmedia skal utføres i hht [Faktaark 34](https://ehelse.no/Documents/Normen/Faktaark%2034%20-%20H%C3%A5ndtering%20av%20lagringsmedia/Faktaark%2034%20-%20H%C3%A5ndtering%20av%20lagringsmedia.pdf) – Håndtering av lagringsmedia.

Bruk av testdata skal følge Normens [Faktaark 43](https://ehelse.no/faktaark-43-bruk-av-testdata-i-systemer-som-inneholder-helse-og-personopplysninger) – Bruk av testdata i systemer som inneholder helse- og personopplysninger.

Produksjonsdata brukt til testformål skal være anonymiserte (Informasjonsklasse 4). I de tilfeller der det ikke er mulig, eller der testens formål ikke oppnås (for eksempel konvertering) ved bruke av anonymiserte data (for eksempel integrasjon og konvertering), skal [Faktaark 48](https://ehelse.no/faktaark-48-informasjonssikkerhet-ved-utforelse-av-testing) – Informasjonssikkerhet ved utførelse av testing etterleves.

## Beskyttelse av data under transport

Normen inneholder flere faktaark som stiller krav til sikring av informasjon under transport. Følgende fakta ark skal følges:

|  |  |
| --- | --- |
| Faktaark | Tittel |
| [Faktaark 24](https://ehelse.no/faktaark-24-kommunikasjon-over-apne-nett) | Kommunikasjon over åpne nett |
| [Faktaark 16](https://ehelse.no/faktaark-16-etablering-av-losning-for-meldingskommunikasjon) | Etablering av løsning for meldingskommunikasjon |
| [Faktaark 29](https://ehelse.no/faktaark-29-hjemmekontor) | Hjemmekontor |
| [Faktaark 20](https://ehelse.no/Documents/Normen/Faktaark%2020%20-%20Sikkerhets-%20og%20samhandlingsarkitektur/Faktaark%2020%20-%20Sikkerhets-%20og%20samhandlingsarkitektur.pdf) | Sikkerhets- og samhandlingsarkitektur |

Kryptering skal benyttes for all informasjon som inneholder personopplysninger når den transporteres over nettverk som HMN ikke har administrativ kontroll over. Dette gjelder om det er informasjon fra sikker sone som er tilgjengeliggjort ved at bruker er tilknyttet intern, åpen eller ekstern sone.

Retningslinje 2 til SP – «Informasjonsflyt mellom soner» spesifiserer mer detaljert kravene til sikring av informasjon under transport.

# Katalogtjeneste

Det skal i HMN benyttes en felles katalogtjeneste. Katalogtjenesten skal benyttes til bruker og klient administrasjon, autentisering og autorisasjon. Alle brukere og klienter skal defineres i katalogtjenesten. Implementering av tekniske «policies» skal gjøres gjennom katalogtjenesten.

**Brukere**
Alle brukere skal ha unike brukerkontoer i katalogtjenesten. Kun i meget spesielle tilfeller kan fellesbrukere aksepteres.

**Klienter**Med klienter menes i denne sammenhengen servere, PCer, skrivere, mobile enheter, osv. (enheter som legges inn i katalogtjenesten).

Alle klienter skal ha en egen maskinkonto i katalogtjenesten.

**Administrator rettigheter for brukere**Brukere skal ikke ha privilegerte administrative rettigheter knyttet til sin brukerkonto. Det gjelder for alle typer brukere. Kun særskilte og godkjente tilfeller kan dette tildeles.

Det skal være egne personlige administratorkontoer for de som trenger administrative rettigheter.

HMN skal ha en tydelig modell for roller og rettigheter (delegeringsmodell).

**Autentisering**Autentisering av brukere skal foregå ved hjelp av definerte attributter. For informasjonsklasse 1 og 3 skal det benyttes PKI og pin-kode for brukerautentisering. For de andre informasjonsklassene kan autentisering foregå ved hjelp av andre attributter, for eksempel brukernavn og passord dersom ikke PKI og pin-kode ikke støttes.

Autentisering i HMN skal følge Normens anbefalinger i [Faktaark 14](https://ehelse.no/Documents/Normen/Faktaark%2014%20-%20Tilgangsstyring/Faktaark%2014%20-%20Tilgangsstyring.pdf) – Tilgangsstyring.

**Federering**
Identiteter i HMNs katalogtjeneste(r) kan federere med identiteter i andre katalogtjenester når dette er hensiktsmessig for å få levert en tjeneste på en god måte til brukerne. I de tilfeller det skal federeres med andre (utenfor HMN) må det være et etablert tillitsforhold som formaliseres gjennom avtaler.
Federering ved innføring og etablering av nye systemer er beskrevet i Retningslinje 3 til SP – «Etablering og endring av tjenester».

**Autorisasjon**Katalogtjenesten skal brukes for å styre brukere og klienters tilgang til ressurser.

# Identitet og sertifikathåndtering

For å understøtte Sikkerhetsplanen skal HMN ha en PKI infrastruktur. HMN benytter to forskjellige sertifikat policier i sine løsninger (nivå 3 og nivå 4[[4]](#footnote-5)). Nivå 3 sertifikater benytter HMN for sterk autentisering mot interne tjenester. Nivå 4 sertifikater benyttes til autentisering og signering mot offentlige tjenester. Tre typer elektroniske sertifikater skal benyttes: person-, maskin- eller virksomhetssertifikater. Det skal være operative «polices» og rutiner for håndtering av alle disse typene sertifikater.

Dokumentet [Strategi for Identitets- og tilgangsstyring](http://eqshemit/cgi-bin/document.pl?pid=hemit&DocumentID=2278) i HMN (EQS) definerer målbildet for identitet og tilgangsstyring i HMN.

For å sikre rettmessig tilgang til interne tjenester skal det eksistere et tilgangssystem som skal kunne autentisere og autorisere brukere. Autorisasjon av brukere kan utføres på forskjellige nivå avhengig av hvilke tjenester det skal gis tilgang til og hvilken autorisasjonsinformasjon IT-systemene er istand til å motta. Det kan omfatte alt fra enkel organisasjonstilhørighet, som for eksempel avdelingstilhørighet, til full autorisasjonsinformasjon.

Tilgangssystemet skal også håndtere all oppretting, oppdatering og avslutning av brukeridentiteter i alle systemer. Denne håndteringen skal i stor grad automatiseres.

## Public Key Infrastructure (PKI)

Det skal eksistere en separat PKI tjeneste med formål utstedelse av elektroniske sertifikater til personer og datamaskiner. I tjenesten skal det eksistere en CA infrastruktur som inngår i CA-kjeden Norsk Helsenett har etablert og forvalter for dette formålet.

PKI basert autentisering skal blant annet benyttes til autentisering av brukere av klientplattformen Puls, samt autentisering av datamaskiner og nettverksutstyr.

[Faktaark 49](https://ehelse.no/Documents/Normen/Faktaark%2049%20-%20Krav%20ved%20bruk%20av%20PKI%20ved%20ekstern%20kommunikasjon/Faktaark%2049%20-%20Krav%20ved%20bruk%20av%20PKI%20ved%20ekstern%20kommunikasjon.pdf) gir en oversikt over grunnleggende krav til bruk av PKI i ekstern kommunikasjon.

## Sertifikathåndtering

Dokumentet [Strategi for Identitets- og tilgangsstyring i HMN](http://eqshemit/cgi-bin/document.pl?pid=hemit&DocumentID=2278) beskriver håndtering av elektroniske sertifikater og smartkort. Se spesielt kapitel 3.3.2 «Forvaltning og bruk av sertifikat og kort med foretakene som kortutsteder (RA)».

Bruk av elektroniske sertifikater skal være i tråd med retningslinjene i «[krav til PKI for offentlig sektor](https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/2010_kravspek_pki_norsk.pdf?id=2156639)» og «[Bruk av PKI med og i offentlig sektor](https://standard.difi.no/forvaltningsstandarder/anvendelsesomraade/standard-for-bruk-av-pki-med-og-i-offentlig-sektor)».

Tabell - Eksempler på bruksområder for sertifikater

|  |  |
| --- | --- |
| **Type elektronisk sertifikat** | **Bruksområde** |
| Kvalifisert personlig sertifikat | Signering av resepter, oppgjørsmeldinger, legeerklæring og sykemeldingerAutentisering av brukere i nasjonal kjernejournal |
| Ikke-kvalifisert personlig sertifikat | Autentisering av brukere i klientplattformen Puls |
| Maskinsertifikat | Autentisering av datamaskinAutentisering av tjeneste på datamaskinKryptering av kommunikasjon med datamaskin |
| Virksomhetssertifikat | Kryptering av meldinger som f.eks henvisning, rekvisisjon, labSignering av meldinger |

Det skal eksistere og forvaltes klare prosesser for utstedelse, fornyelse, tilbaketrekking og transport av elektroniske sertifikater med tilhørende nøkler.

# Eksterne tjenester

Med eksterne tjenester menes IT tjenester som blir gjort tilgjengelige i ekstern tjenestesøyle. Disse tjenestene er ikke nødvendigvis plassert innenfor et fysisk område som HMN har kontroll over. De kan for eksempel være plassert hos en tredjepart/tjenesteleverandør eller i skyen.

De samme policies og retningslinjer skal gjelde for slike tjenester som i andre tjenestesøyler.

Retningslinje 3 til SP – «Etablering og endring av tjenester» og Retningslinje 5 til SP - «Bruk av skytjenester» gir videre retningslinjer og hjelp til bruk av eksterne tjenester.

# Konfigurasjonskontroll

Konfigurasjonsstyring skal sørge for at IT infrastruktur og systemer til enhver tid er konfigurert i tråd med gjeldende konfigurasjonsstandard.

Det skal eksistere en forankret konfigurasjonsstandard og tilhørende arbeidsprosesser som sørger for en helhetlig oppdatering av en sentral konfigurasjonsdatabase. Avviket mellom standard og reell konfigurasjon skal utbedres ved å gjennomføre tiltak som er behandlet av gjeldende endringsprosess.

Tilfredsstillende konfigurasjonsstyring er basert på at det skal eksistere en felles konfigurasjonsdatabase som inneholder oppdatert konfigurasjonsinformasjon for IT infrastruktur og systemer. Den skal inneholde konfigurasjonselementer (CI-configuration items) som beskriver konfigurasjon av IT infrastruktur og systemer, relasjoner mellom konfigurasjonselementer, verdikjeder og konfigurasjonselementers integrasjon med tjenesteavtaler. Alle datakilder som inneholder konfigurasjonsinformasjon skal oppdateres i konfigurasjonsdatabasen.

Kravet til konfigurasjonsinformasjonens integritet er høy og krever at alle arbeidsprosesser (ITIL) som endrer konfigurasjon skal oppdatere konfigurasjonsinformasjonen når endringene gjennomføres.

Konfigurasjonsdatabasen skal i størst mulig grad oppdateres automatisk for å oppnå størst mulig integritet til enhver tid. Manuelle oppdateringer er likevel nødvendig for å oppdatere relasjoner og verdikjeder. Det skal derfor utpekes ansvarlige eiere av konfigurasjonsinformasjon og sørges for at arbeidsrutiner og prosesser er tilpasset god forvaltning av konfigurasjonsinformasjon.

Oppdateringstiltak er avhengig av at det til enhver tid eksisterer en konfigurasjonsdatabase som inneholder informasjon om alle enheter i IT infrastrukturen, systemene disse produserer og tilhørende konfigurasjonselementer.

Trusselsituasjonen for IT infrastruktur og systemer forverrer seg stadig og nye sårbarheter avsløres og angripes. Når en slik hendelse oppstår skal det raskt gjennomføres tiltak som utbedrer sårbarheter i IT infrastruktur og systemer ved å benytte tilgjengelig konfigurasjonsinformasjon i konfigurasjonsdatabasen. Tiltakene skal gjennomføres ved å benytte gjeldende endringsprosess og rutiner for å håndtere hendelser.

Produksjon av IT tjenester skal foregå på IT infrastruktur og systemer som kjører lisensiert programvare med gyldig supportavtaler. Det skal eksistere en forvaltningsprosess som holder rede på og varsler utløp av lisenser og supportavtaler. Den skal regelmessig gjennomløpe konfigurasjonsdatabasen og varsle systemeier ved utløp. Varslingen skal skje tilstrekkelig lenge før utløp slik at systemeier har tid til å anskaffe innsatsmidler tilstrekkelig til å gjennomføre oppgraderingen.

Implementering av nye enheter i IT infrastrukturen skal gjennomføres ved at det installeres et godkjent og standardisert operativsystem på datamaskinen, med en tilhørende herdingskonfigurasjon og sørge for at det skjer en automatisk oppdatering av konfigurasjonsdatabasen.

Distribuert og personavhengig informasjon om elektroniske sertifikater og deres utløpstid er en risiko for fortløpende produksjon av IT tjenester. Informasjon om elektroniske sertifikater skal derfor legges inn i konfigurasjonsdatabasen og det skal eksistere en tilpasset forvaltningsprosess som varsler sertifikateier minst 90 dager før sertifikatet utløper.

# Infrastruktursikkerhet

Alle elementer som inngår i leveransen av en tjeneste skal gjennomgå en helhetlig sikring.

Alle IT-systemer skal herdes i tråd IT-systemets rolle og plassering. Retningslinje 6 til SP – «Herding av servere», Retningslinje 7 til SP – «Herding av nettverkskomponenter» og Retningslinje 8 til SP – «Herding av klienter» beskriver nærmere beste praksis.

Det skal kun benyttes versjoner av operativsystemer som vedlikeholdes av programvareleverandør.

## Nettverksinfrastruktursikkerhet

All tilgang til nettverksenheter skal kun gis til autoriserte og autentiserte brukere. Påloggingssesjonen skal være kryptert og en felles brukerdatabase som er tilkoblet sentral katalogtjeneste skal benyttes.

All tilgang til nettverksenheter skal logges, slik at krav til sporbarhet tilfredsstilles.

Alle nettverksenheter skal være herdet etter beste praksis og tjenester som ikke brukes skal deaktiveres. Se Retningslinje 7 til SP – «Herding av nettverkskomponenter» for mer informasjon.

Tilgang til celler i nettverket skal sikres og det skal kun gis tilgang for autentisert og autorisert utstyr og brukere. Autentisering skal primært være sertifikatbasert (802.1x). Utstyr det ikke er mulig å autentisere eller autorisere, vil få en tvungen tilknytning til et karantenenettverk med et svært begrenset tjenesteutvalg.

## Serversikkerhet

Alle servere skal herdes, sikres med antivirus tjeneste, sikkerhetspatches og innlemmes i HEMITs driftsløsninger.

### Serversikring

Alle servere fra og med Microsoft Windows Server 2012:

* med nettverkstilgang til sikker sone skal være typegodkjent av Produktrådet for denne type tilgang og ha standard konfigurasjon
* skal være underlagt sentral konfigurasjonskontroll og overvåking
* skal ha antivirus installert, med virusdefinisjonsfiler fra en sentral enhet
* skal kun benytte operativsystem som vedlikeholdes av programvareleverandøren
	+ Avvik fra dette kan tillates, men må da ha vært gjenstand for en individuell risikovurdering
* skal sikres og herdes i tråd med Retningslinje 6 til SP – «Herding av servere»
* skal benytte IDS løsninger og eventuelt elektroniske sertifikater (PKI) og IPSEC hvis IT-systemet er eksponert i usikre soner, for eksempel DMZ.

### Patching

Alle servere som inngår i HMNs infrastruktur skal underlegges et regime for sikkerhetspatching. Dette er nærmere beskrevet i Retningslinje 6 til SP – «Herding av servere».

## Klientsikkerhet

Alle klienter som skal koble seg til HMNs infrastruktur skal beskyttes med antivirus og innlemmes i HEMITs driftsløsninger. Sikringen skal også innbefatte herding (se Retningslinje 8 til SP – «Herding av klient»), patching og andre nødvendige tiltak.

Graden av sikring vurderes ut fra hvilken celle klienten skal koble seg til.

### Klientsikring

Alle klienter

* med nettverkstilgang til sikker sone skal være typegodkjent av Produktrådet for denne type tilgang og ha standard konfigurasjon
* skal være underlagt sentral konfigurasjonskontroll og overvåking
* skal ha antivirus installert og virusdefinisjonsfiler skal hentes fra en sentral enhet
* skal kun benytte operativsystem som vedlikeholdes av programvareleverandøren
	+ Avvik fra dette kan tillates, men må da ha vært gjenstand for en individuell risikovurdering
* skal sikres og herdes i tråd med Retningslinje 8 til SP – «Herding av klienter»

Prinsipielt gjelder det samme for nettverkstilgang til intern sone, men i denne sonen kan det være løsninger som kompenserer for noen av punktene over. Det kan for eksempel være løsninger som er implementert for at brukere skal kunne ta med egne/private klienter for bruk i jobb sammenheng (BYOD).

### Elektromedisinsk utstyr (MU)

Elektromedisinsk utstyr/systemer som ikke tilfredsstiller kravene i Kapittel 14.3.1 kan likevel innplasseres i HMNs infrastruktur, forutsatt at alle krav stilt i Kapittel 16.2 og Retningslinje 3 til SP – «Endring og etablering av tjenester» innfris.

### Mobilt utstyr

Med mobilt utstyr menes bærbar PC, mobiltelefon, nettbrett, digitalt kamera og video og lignende som brukes av ansatte i arbeidet.

Det stilles samme krav til mobilt utstyr som til andre klienter.

# Sporbarhet og logghåndtering

Sporbarhet og logging skal være implementert i henhold til Norm for Informasjonssikkerhet, [Faktaark 15](https://ehelse.no/faktaark-15-logging-og-oppfolging-av-logger). I tillegg gjelder [Faktaark 47 – Autorisasjonsregistre](https://ehelse.no/Documents/Normen/Faktaark%2047%20-%20Autorisasjonsregister/Faktaark%2047%20-%20Autorisasjonsregister.pdf) for IT-systemer som behandler helse- og personopplysninger og brukertilganger for å sikre den registrertes rettigheter. (Innsyn i hvem som har hatt innsyn i opplysningen, når).

For informasjon som ikke direkte omfattes av Normen skal logger oppbevares i 3 måneder. Det gjelder alle informasjonsklasser utover informasjonsklasse 1 og inkluderer alle driftslogger.

I enkelte tilfeller og for enkelte systemer kan det besluttes at logger skal oppbevares lengre enn 3 måneder.

Alt som kan påvirke tjenesteproduksjonen i HMN på en negativ måte skal logges. Det kan for eksempel være systemlogger fra infrastruktur, logging av internettrafikk, logging av tilganger til driftssystemer og så videre.

# Systemvurderinger/godkjenninger

Nye IT-systemer eller endringer i eksisterende IT-systemer som har betydning for informasjonssikkerheten, skal klassifiseres (jfr. kapittel 2), risikovurderes, godkjennes og innplasseres i tjenestenivå.

## Risikovurdering

IT-systemer som skal etableres i HMNs IT-infrastruktur skal gjennomgå en RoS-analyse (risikovurdering) i designfasen og før driftsettelse. Ved endringer på IT-systemer skal en ny RoS-analyse gjennomføres. RoS-analyse skal gjennomføres i henhold til [Faktaark 7](https://ehelse.no/faktaark-07-risikovurdering).

Negativ risiko kan håndteres på ulike måter

* Overføres
* Aksepteres
* Unngås
* Redusere sannsynlighet
* Minimere konsekvens

En handlingsplan utarbeides med definerte tiltak og en ansvarlig for ikke-akseptabel risikoer.

* Aksepterte risikoer som er utenfor akseptgrensenene skal begrunnes
* Risikoer skal prioriteres og håndteres deretter
* Tiltak gjennomføres i henhold til handlingsplan.

For celler som innbefatter MU skal “*IEC 80001-1,* Application of risk management for IT-networks incorporating medical devices” følges. Denne bidrar til å etablere risikohåndtering tilpasset IT-nettverk som omfatter MTU.

## Godkjenninger

Designdokumentasjon og risikovurdering skal danne grunnlaget for en godkjenning av IT-systemer som skal innføres eller endres. Det er Arkitekturforum som anbefaler løsningene.

# Tjenestenivåer

Klassifisering av IT-systemers prioritet er med på å avgjøre hvilket tjenestenivå en løsning skal leveres i tråd med. Tjenestenivåer (SLA) i HMN er definert i Vedlegg 2 til Avtale om tjenester.

## Redundans i infrastruktur (nett, bygninger, strøm, kjøling)

Redundans i infrastruktur er grunnleggende for å kunne levere de tjenestenivåer som er avtalt med kundene.

Alle kritiske funksjoner skal dubleres for å sikre høy tilgjengelighet på alle kommunikasjonstjenester. Dette gjelder både byggtekniske- (strøm, kjøling, føringsveier osv) og nettverksinfrastruktur-løsninger (sikkerhetsbarrierer, VPN-terminering, brannmurer, svitsjer osv).

Det skal også for tjenestemaskiner/servere som produserer tjenester med de høyeste prioriteter være:

* Dublerte tilknytninger til infrastrukturen for å sikre høy tilgjengelighet på tjenestene
* Dublering av kritiske komponenter
* Dublerte komponenter skal plasseres i forskjellige datarom

Dokumentet “Krav til datarom” og “Krav til koblingsrom” beskriver kravene som stilles til datarommene som skal levere tjenester i tråd med tjenesteavtalen, koblings og kommunikasjonsrom.

## – Beredskap

Det skal til enhver tid være utarbeidet beredskapsplaner for IT i HMN. Disse finnes i EQS under Beredskap og Sikkerhet.

## – Reservedrift

Ved bortfall av kritiske løsninger og komponenter skal det være lagt opp til reservedrift. Omfanget og metoden for reservedrift må kartlegges i RoS-analyse for løsningen, og avtales med kunden for hvert enkelt system.

## – Overvåkning

All underliggende infrastruktur og kritiske løsninger skal overvåkes. Det skal for hver komponent eller løsning være definerte tiltak ved bortfall/feil.

For tjenester og løsninger levert til kunden må overvåking og tiltak gjenspeile de tjenestenivåer (SLA) som er avtalt for tjenesten. OLA må også gjenspeile de SLA som er avtalt med kunden.

## - Backup/restore

Det skal for alle løsninger finnes installasjonsdokumentasjon og planer for ”disaster recovery”. Omfanget av disse må gjenspeile tjenestenivået (SLA) som er avtalt med kunden.

Kritiske komponenter og løsninger skal være underlagt konfigurasjonskontroll, for å ivareta en rask re-etablering ved bortfall/feil.

1. Med informasjon menes i SP informasjon innenfor alle Informasjonsklasser (jfr kap 2 – Klassifisering av systemer). [↑](#footnote-ref-2)
2. Ref. [LOV-2000-04-14-31](http://www.lovdata.no/cgi-wift/wiftldles?doc=/app/gratis/www/docroot/all/nl-20000414-031.html&emne=personopplysning*&&) Personopplysningsloven [↑](#footnote-ref-3)
3. Datasenter kan være plassert ute hos helseforetakene og ikke nødvendigvis i HEMIT sitt sentrale datasenter i Trondheim. Slike datasenter skal være underlagt samme sikkerhetskrav som det sentrale datasenteret. [↑](#footnote-ref-4)
4. Nivå 4 defineres i [Kravspesifikasjon for PKI i offentlig sektor](https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/), som er hjemlet i [eForvaltningsforskriften](https://lovdata.no/dokument/SF/forskrift/2004-06-25-988). [↑](#footnote-ref-5)