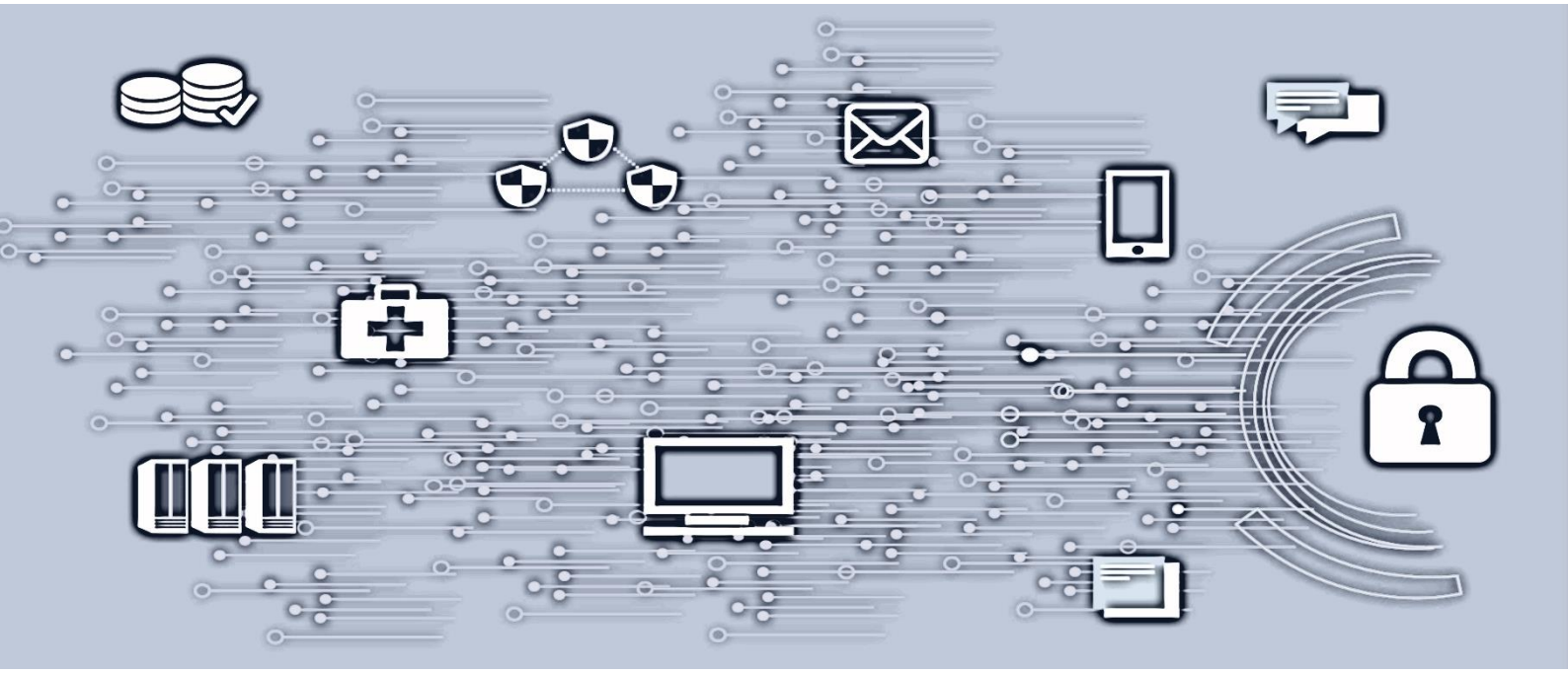
SYKEHUSPARTNER

Policy for Regional Sonemodell



1 Innhold

Versjon	Dato	Godkjent av
1.0	04.22.22	ISMB
1.1	23.09.23	ISMB

1. Hensikt og omfang

Dette dokumentet er en felles regional policy som definerer regional sonemodell. Policyen er rettet til Sykehuspartner for bruk ved implementasjon og styring av IKT-tjenester i Helse Sør-Øst.

1.1 Dokumentforvaltning

Dette dokumentet inngår i Sykehuspartner HFs ledelsessystem og regionale bruksvilkår for informasjonssikkerhet.

1.2 Målgruppe

Målgruppen for dokumentet er de som arbeider med direkte eller indirekte med tekniske løsninger knyttet til nettverkssegregering. Dette kan være; men ikke begrenset til:

- IT-teknisk driftspersonell
- Nettverksanalytikere
- Løsningsarkitekter
- Rådgivere som utfører risiko- og sårbarhetsvurderinger
- Sikkerhetsrevisorer
- Prosjektledere i moderniseringsprosjekter

2. Definisjoner

Sykehuspartner vedlikeholder en ordbok i kvalitetsportalen som inneholder definisjoner av begreper og forkortelser. Under er det listet opp noen sentrale dokumenter som brukes i denne policyen. Oppdatert versjon av definisjoner ligger i ordboken i Sykehuspartner sin kvalitetsportal (intern lenke).

- **Administrasjonsplan:** Administrasjonsplanet etablerer kjøremiljø på bestilling fra kontrollplanet. Administrasjonsplanet inneholder administrative grensesnitt for byggeklosser i infrastruktur/plattform; som nettverk, sikkerhet, lagring, server.
- **Dataplan**: Dataplanet benyttes eksempelvis for administrative og kliniske applikasjoner. Dataplanet etableres av administrasjonsplanet, og styres av kontrollplanet.
- **Funksjonsdomene:** En logisk avgrenset del av felles plattform som er opprettet for en spesifikk tenant eller funksjon. I Sykehuspartner skilles det mellom "Regionalt funksjonsdomene" for funksjon eller tjenester med felles dataansvar, og "HF-spesifikt funksjonsdomene" for spesifikt juridisk foretak med separat dataansvar.
- **Kontekst**: I «Sikkerhetsstrategi for Sykehuspartner» er det besluttet en klassifiseringsmodell som deler informasjon inn i fire nivåer. Disse nivåene omtales som «kontekster».
- **Kontrollplan**: Kontrollplanet sørger for at kjøremiljøene fungerer og leverer riktig kvalitet og informasjonssikkerhet. Kontrollplanet inneholder verktøy for drift og forvaltning av plattformen.
- **Mikrosegmentering**: En praksis for virtuell segmentering i soner. Disse sonene tilbyr isolasjon av informasjonsverdier og systemer som bedrer informasjonssikkerheten blant annet ved å redusere negative effekter av skadevare og uhell.
- **Perimetersikring**: Dette beskriver en sikkerhetsmekanisme for å sikre grensesnitt mot eksempelvis en sone, et funksjonsdomene, eller et miljø.
- **Sone**: Soner benyttes som et grunnleggende prinsipp i sikkerhetsarkitekturen. En sone utgjør en del av et informasjonssystem og kan blant annet være en fysisk eller logisk separert del av et nettverk, eksempelvis opprettet ved behov for skjerming av personopplysninger.
- **Tenant**: En separat juridisk enhet med selvstendig dataansvar, juridisk enhet, virksomhet.
- **CERT**: Funksjonsdomene for CERT (Computer Emergency Response TEAM).

- **DMZ**: Funksjonsdomene for etablering av tjenester for ekstern kommunikasjon.
- **Basistjenester**: Funksjonsdomene for Basis infrastrukturtjenester.
- **Integrasjonstjenester**: Funksjonsdomene med tjenester for sikker integrasjon mellom andre funksjonsdomener; mottak, mellomlagring og videresending.
- **Fellestjenester**: Funksjonsdomene for etablering av regionale tjenester med delt dataansvar mellom 2 eller flere HF.
- **FD_<HF, kortnavn>**: Funksjonsdomener opprettet for spesifikke virksomheter.. For etablering av HF-spesifikke tjenester med eget dataansvar.

3. Formål

3.1 Ansvar

Dataansvarlig har ansvar for all behandling av helse- og personopplysninger med tilknytning til virksomheten. Administrerende Direktør har ansvar for at alle personopplysninger blir behandlet iht. gjeldende lovverk, se spesielt pasientjournalloven, helseberedskapsloven, helseregisterloven og personopplysningsloven, samt norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen).

Sykehuspartner HF er regionens primære databehandler. I tillegg til de regionalt vedtatte dokumentene i det fellesregionale ledelsessystemet for informasjonssikkerhet, er Sykehuspartner HF ansvarlig for de regionale bruksvilkår for informasjonssikkerhet som foretakene må akseptere.

Sykehuspartner HF følger det regionale ledelsessystemet for informasjonssikkerhet.

Ledere på alle relevante nivåer har ansvar for oppfylling av dokumentet i egen enhet.

3.2 Omfang

Denne policyen definerer et rammeverk for implementasjon, drift og vedlikehold av funksjonsdomener og soner i IKT-leveranser i Helse Sør-Øst. Dette skal sikre et godt grunnlag for etterlevelse av krav til informasjonssikkerhet og personvern, samt sikre effektiv styring av teknisk infrastruktur.

Denne modellen legges til grunn for all IT-arkitektur og alle IKT-leveranser i Helse Sør-Øst, men den har ikke tilbakevirkende kraft.

Det skal legges til rette for kommunikasjon på tvers av gamle og nye plattformer.

4. Sikkerhetskrav

4.1 Innledning

Personvern- og informasjonssikkerhet skal ivaretas på best mulig måte i modernisering av teknisk infrastruktur. Dette dokumentet stiller overordnede og prinsipielle krav til hvordan en sonemodell og tilknyttede sikkerhetsmekanismer skal etableres. Det skal etableres veileder for mer detaljert beskrivelse av modellen, for implementering for forvaltning.

4.2 Regional Sonemodell

Regional sonemodell definerer et strukturert økosystem for IT tjenester for å oppnå målsetningene som ble beskrevet innledningsvis.

Et viktig overordnet mål for sonemodellen er å bidra til høy grad av konfidensialitet, integritet og tilgjengelighet, samt tillit i alle deler av alle organisasjoner i Helse Sør-Øst.

Fokus i denne policyen er å sikre at informasjon:

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

Modellen skal ta høyde for at HSØ omfatter flere juridiske enheter med selvstendige dataansvar, samt eventuelt tilsvarende eksterne juridiske enheter. Hver for seg behandler disse enhetene informasjon av særlig sensitiv karakter på høyeste nivå, kontekst 4, beskrevet i NO-6 – Sikkerhetsstrategi, under veiledende dokumenter, kap. 4.2.8 *Klassifisering av informasjon.*

Type informasjon	Maksimal konsekvens	Relevante kriteria fra Styringssystem for informasjonssikkerhet
Sensitive personopplysninger Virksomhetskritisk informasjon	4 - RØD	Hendelsen medfører tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse/integritet. Hendelsen medfører manglende respekt for den enkeltes liv, integritet eller menneskeverd.
Personopplysninger, inkludert fødselsnummer Virksomhetssensitive opplysninger	3 - ORANSJE	Hendelsen medfører helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse/integritet. Hendelsen medfører manglende tillit mellom pasient og helsevesen-/personell. Hendelsen medfører helsehjelp med utilstrekkelig kvalitet.
Intern informasjon	2 - GUL	Hendelsen medfører at personlig integritet og privatlivets fred ikke ivaretas. Hendelsen medfører helsehjelp med utilstrekkelig kvalitet. Hendelsen medfører betydelig økonomisk tap som kan gjenopprettes, eller tap av anseelse/integritet gjennom kompromittering av krenkende opplysninger.
Åpen informasjon	1 - GRØNN	

Figur 1 Helse Sør-Øst klassifiseringsmodell for informasjon.

4.2.1 Integritet i plattformene

Plattformene består av funksjonsdomener for kontroll- og administrasjonsplan, samt ett eller flere dataplan for andre funksjonsdomener for kunderettede applikasjoner og tjenester.
Funksjonsdomenene Administrasjonsplan og Kontrollplan har sentrale funksjoner i plattformen, og

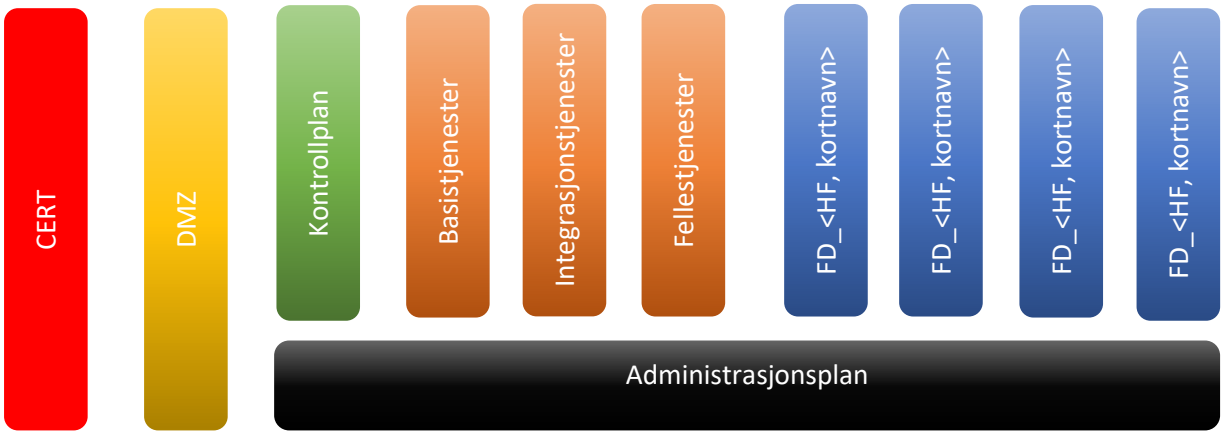
integriteten i disse vil være avgjørende også for andre deler av plattformen. Både Funksjonsdomenene Administrasjonsplan og Kontrollplan skal beskyttes spesielt og ha et svært restriktivt regime for tilgang.

Sporbarhet knyttet til systemendringer i plattformen skal ivaretas med løsning for privilegert tilgang som eneste vei inn for å understøtte spesiell beskyttelse i Administrasjonsplan og Kontrollplan, inkludert monitorering av tilgang og aktivitet. I de tilfeller der løsning for privilegert tilgang ikke kan benyttes skal tilgang begrenses og sikres på annet vis for å ivareta integriteten i plattformen. Se for øvrig NO-50-Policy for funksjonsdomenene kontroll- og administrasjonsplan for mer detaljer.

Integritet i plattformene er vesentlig for å understøtte at konfidensialitet og tilgjengelighet kan ivaretas godt nok, ved at god ivaretakelse av integritetsaspektet medfører at uautoriserte endringer ikke kan gjennomføres.

4.2.2 Funksjonsdomene

Funksjonsdomener er øverste nivå og en logisk struktur. Sikkerhetspolicy for regional sonemodell definerer et sett med funksjonsdomener for funksjon og ett sett med funksjonsdomener per virksomhet.



Figur 2 Prinsipiell fremstilling av funksjonsdomener i regional sonemodell.

Føringer for funksjonsdomener

- Funksjonsdomener skal være logisk separert fra andre hverandre.
- Funksjonsdomener skal opprettes i henhold til Figur 2 over:
  - Funksjonsdomener for funksjoner.
  - Funksjonsdomener per virksomhet.
- Ved behov for funksjonsdomener som ikke inngår i den skisserte modellen i Figur 2 over skal dette godkjennes av SPHF sikkerhet.
- Et funksjonsdomene skal ha perimetersikring og all kommunikasjon til og fra funksjonsdomene skal gå gjennom denne.
- Kommunikasjon mellom funksjonsdomener skal autentiseres og autoriseres via fellesregional autentiseringstjeneste (IAM/IDM), eller på annet vis ivareta integriteten og sikkerhet i funksjonsdomenene.
- Et funksjonsdomene kan instansieres flere ganger, som på forskjellige lokasjoner.

- Alle instanser av samme funksjonsdomene kan kommunisere med hverandre.
- Et funksjonsdomene skal legge til rette for andre miljø enn produksjon.

4.2.3 Sone

Funksjonsdomener skal deles opp i mindre segmenter av lignende tjenester, kalt soner.

Føringer for soner

- En sone skal tilhøre ett funksjonsdomene.
- Soner skal være logisk separert fra hverandre.
- Alle soner skal omkranses og beskyttes av funksjonsdomene.
- En sone skal benytte mikrosegmentering og perimetersikring per host. Dersom dette ikke er mulig skal andre tilsvarende teknikker for sikring benyttes, som segmentering per tjeneste.

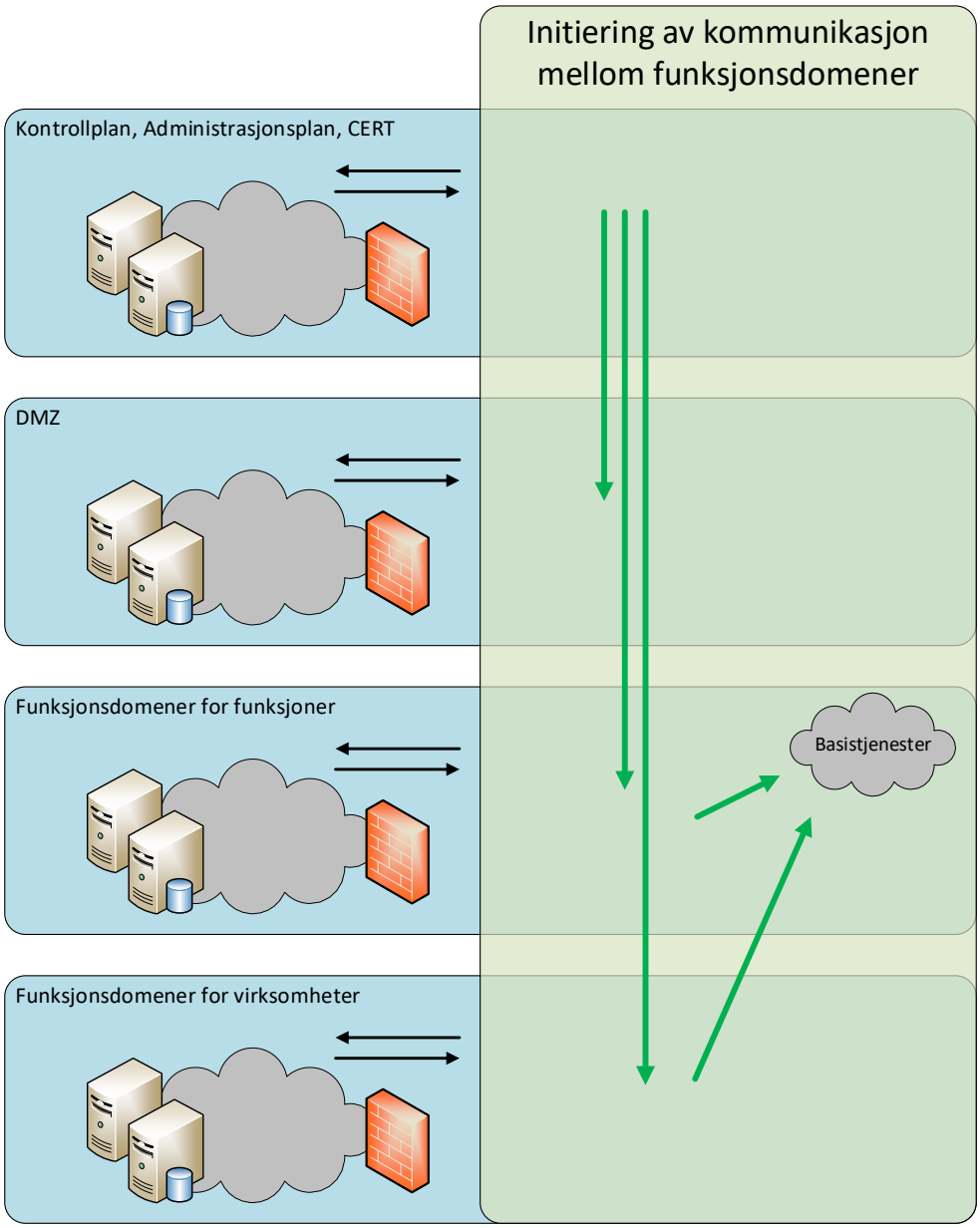
4.3 Sonemodell i Datasenter

Med datasenter menes digital tjenesteproduksjon i IKT-rom som definert i Målbilde lokale IKT rom i Helse Sør-Øst (intern lenke i Sykehuspartner) eller sky, knyttet til moderniseringsprogrammet STIM og senere. Datasenter kan være driftet av Sykehuspartner eller tjenesteutsatt, og infrastrukturen kan være både fysisk og virtuell.

4.3.1 Krav til sonemodell

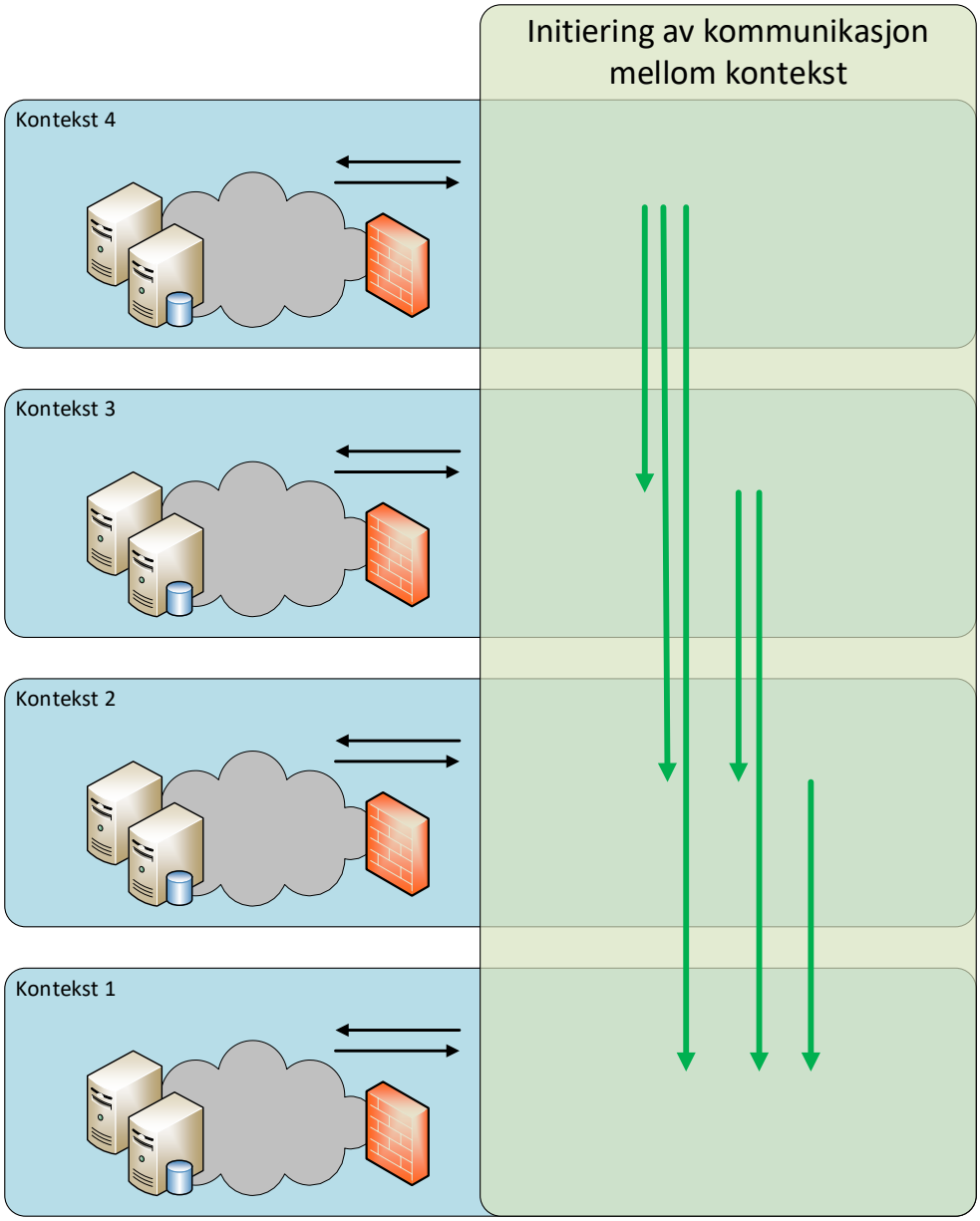
Sonemodell skal organiseres som funksjonsdomener med tilhørende soner.

- Kommunikasjon på tvers av funksjonsdomener og soner skal krypteres i henhold til kryptopolicy, NO-POLICY-15 - Fellesregional kryptopolicy.docx (fisp.no)
- Kommunikasjon mellom funksjonsdomener (Figur 3)
    - Alle soner i funksjonsdomenene Kontrollplan, Administrasjonsplan og CERT kan kommunisere med alle soner i andre funksjonsdomener.
    - Annen kommunikasjon relatert til Kontroll- og Administrasjonsplan er regulert i «Policy for funksjonsdomenene kontroll- og administrasjonsplan».
    - Alle soner i funksjonsdomenene Integrasjonstjenester, Fellestjeneste, samt viksomhetsspesifikke funksjonsdomener kan kommunisere med funksjonsdomene Basistjenester.
    - Kommunikasjon mellom forskjellige funksjonsdomener skal gå via en sone for integrasjon.



Figur 3 Prinsipper for initiering av kommunikasjon mellom funksjonsdomener

- Kommunikasjon mellom kontekst (Figur 4)
  - Kommunikasjon internt innen samme applikasjon er tillatt mellom kontekster.
  - En sone skal ikke initiere kommunikasjon med sone i høyere kontekst enn seg selv. Informasjonsflyt skal kun gå mellom soner i tilsvarende kontekst eller initieres fra høyere nivå og ned, beskrevet i NO-6 – Sikkerhetsstrategi. Unntatt fra dette er kommunikasjon fra funksjonsdomenene Kontrollplan, Administrasjonsplan og CERT.



Figur 4 Prinsipper for initiering av kommunikasjon mellom kontekst

4.4 Sonemodell for Konsument

Med konsument menes klient som konsumerer IT tjenester levert i datasenter som definert over.

Klient kan være, men ikke begrenset til

- Enhet/bruker som er koblet til nettverk på en HSØ lokasjon.
- Enhet/bruker som er koblet til gjennom VPN-løsning i HSØ.
- Enhet/bruker som er koblet til gjennom Citrix-løsning i HSØ.
- Enhet/bruker fra internett

4.4.1 Krav til sonemodell

Sonemodell skal organiseres som funksjonsdomener med tilhørende soner.

- Kommunikasjon på tvers av soner og funksjonsdomener skal krypteres i henhold til kryptopolicy, NO-POLICY-15 - Fellesregional kryptopolicy.docx (fisp.no)
- Konsumenter skal knyttes til funksjonsdomener basert på lokasjon og/eller autentisering.
- Konsumenter skal grupperes i soner basert på egenskaper.

4.5 Realisering av sonemodell

Det skal etableres en tilhørende veiledning for å beskrive modellen mer detaljert, for implementering for forvaltning.

5. Forvaltning av regional sonemodell

5.1 Endringshåndtering

Endringer skal håndteres i henhold til enhver tid gjeldende endringsprosess (link fungerer kun internt i SPHF).

5.2 Avvikshåndtering

Det kan oppstå tilfelle hvor man ikke er i stand til å etterleve krav i denne policy. I slike tilfeller skal dette komme tydelig frem i design og ros, og håndteres i henhold til gjeldende prosess.

6. Referanser

- Helse Sør-Øst – Styringssystem for informasjonssikkerhet
  - Sikkerhetsstrategi med supporterende dokumenter
  - Sikkerhetsinstruks med supporterende dokumenter
- Personvernforordningens artikkel 32 om sikkerhet ved behandlingen, og helseregisterlovens § 21 om sikring av personopplysninger.
- Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren (Normen.no)
- NO-50-Policy for funksjonsdomenene kontroll- og administrasjonsplan
- Endringsprosess