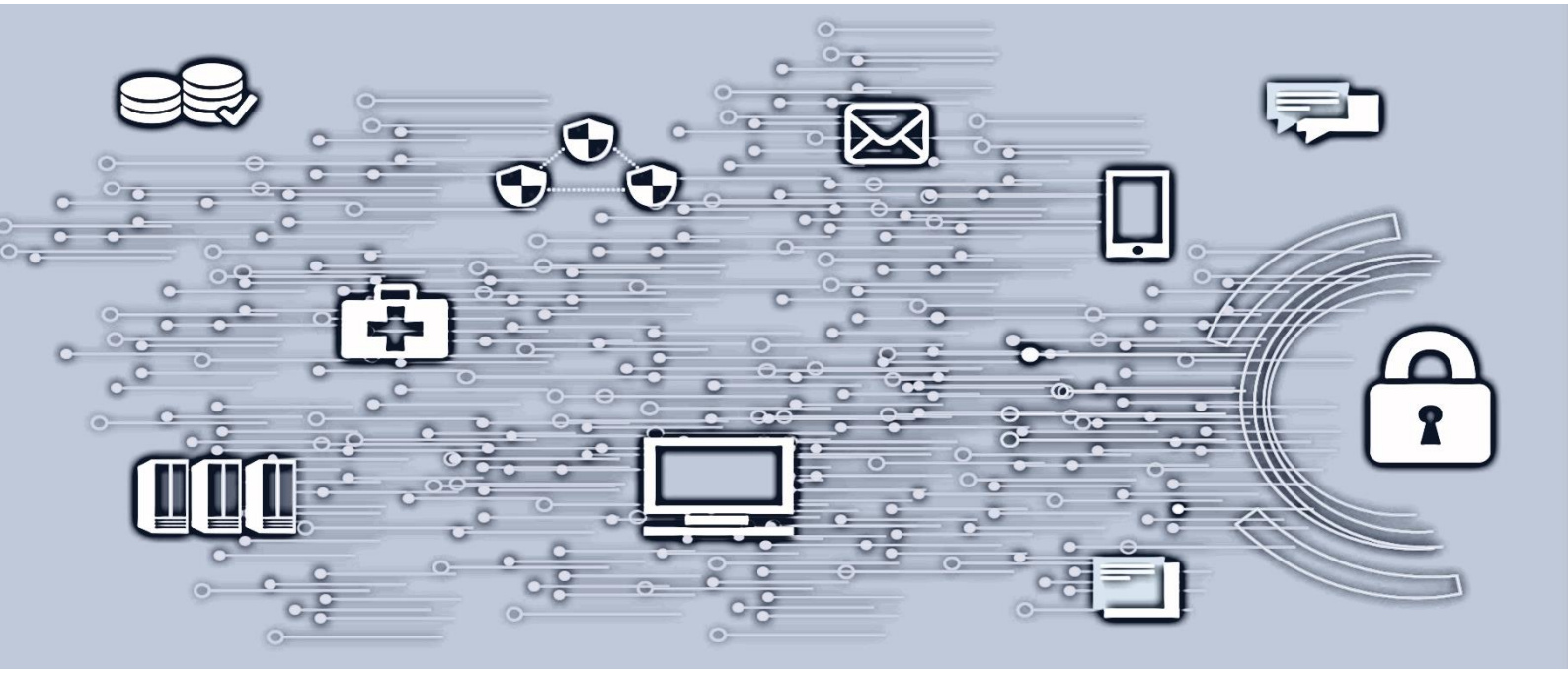
SYKEHUSPARTNER

Regional autentiseringspolicy for helseforetakene i Helse Sør-Øst



Intern

Versjon	Dato	Godkjent av
1.0	2016-12-22	Christian Jacobsen
1.1	2018-10-23	
1.2	2021-04-15	Øyvind Grinde
1.3	2022-03-04	Christian Jacobsen
1.4	2022-09-23	Christian Jacobsen
1.5	2023-09-01	Informasjonssikkerhetsleder

1. Hensikt, omfang og definisjoner

1.1 Hensikt

Denne policyen har som formål å sikre at medarbeidere i Helse Sør-Øst er informert om og forstår kravene knyttet til autentisering for organisasjonens IKT-systemer.
Målet er å sikre en sterk og pålitelig autentiseringsprosess som tilfredsstiller de dynamiske og stadig skiftende behovene og standardene innen informasjonssikkerhet.

1.2 Omfang

Denne policyen er utformet for å fungere som en veileder og et styringsdokument for utvikling og implementering av nye tjenester. Den skal bidra til å sikre at autentiseringsprosesser er tilrettelagt på en sikker og effektiv måte, i tråd med beste praksis.
Eksisterende tjenester er ikke pålagt å innfri de nye kravene til autentisering som er beskrevet i denne policyen.
Ved fremtidige oppdateringer, modifikasjoner eller endringer av tjenestene, er det et absolutt krav å revidere, oppdatere og forbedre autentiseringen i henhold til denne policyen. Dette kravet er nødvendig for å opprettholde et høyt sikkerhetsnivå og for å beskytte organisasjonens data og systemer mot uautorisert tilgang.
Dersom disse kravene ikke blir fulgt ved oppdatering av tjenester, skal det rapporteres som avvik.
Ved avvik skal løsningsdesign og/eller ROS (risiko og sårbarhetsanalyse) for aktuell tjeneste beskrive hvorfor avviket er nødvendig.

1.3 Definisjoner

Autentisering er prosessen der et system eller en tjeneste bekrefter en brukers påståtte identitet ved å verifisere presenterte legitimasjonsopplysninger mot tidligere etablerte, lagrede legitimasjonsopplysninger. Dette innebærer å kontrollere at brukeren faktisk er den de hevder å være ved hjelp av en eller flere autentiseringsfaktorer. Formålet med autentisering er å beskytte systemer og data ved å begrense tilgangen til autoriserte brukere og hindre uautorisert tilgang.

Active Directory (AD) er en Microsoft-utviklet katalogtjeneste som sentraliserer informasjon om nettverksressurser som brukerkontoer og datamaskiner. AD organiserer disse ressursene, muliggjør autentisering og autorisasjon innenfor et nettverk, og støtter Single Sign-On (SSO) for enklere tilgang til flere applikasjoner med én autentisering.

BAT er nettbutikken til IDM og gir mulighet for automatisk tilgangsstyring både for tildeling og fjerning av tilganger. FAQ: BAT - Bestilling av tilganger (fisp.no)

Min Sykehuspartner er vår selvhjelpsportal. Her finnes blant annet:

- Lenke til tilgangsportalen BAT
- Veiledninger - slik at problemer kan løses på egen hånd
- Kontaktskjema som kan benyttes ved behov for hjelp eller ved opplevde feil

- Lenke til utstyr som kan bestilles i Varekatalogen
- Bestillingsskjema

FIDO2 er en standard for passordløs autentisering som gir en sikker og brukervennlig måte å bekrefte brukeridentitet på. Autentiseringsnivå på FIDO2-løsninger baserer seg på godkjenning fra NKOM. Elektronisk identifikasjon (eID) - Nkom

Mobilbasert MFA (Multi-Faktor Autentisering) er en autentiseringsmetode som krever to eller flere uavhengige faktorer for å verifisere en brukers identitet. En av disse faktorene er typisk en bekreftelse som blir generert på brukerens mobile enhet, noe som gir et ekstra sikkerhetslag utover tradisjonell brukernavn- og passordverifisering.

2. Ansvarlige

- Administrerende direktør har ansvar for at alle personopplysninger blir behandlet iht. gjeldende lovverk, se spesielt pasientjournalloven (Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) - Lovdata), helseregisterloven (Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) - Lovdata) personopplysningsloven med forskrift Lov om behandling av personopplysninger (personopplysningsloven) - Lovdata
- Ledere på alle nivåer har ansvar for oppfylling av instruksen i egen enhet.
- Personell som i kraft av sin stilling ved virksomheten har tilgang til helse- og personopplysninger inkludert journal, plikter å etterleve dette dokumentet.

3. Autentisering i Helse Sør-Øst

Helse Sør-Øst benytter PingFederate (regional autentiseringstjeneste) som er et identitets- og fødereringsprodukt. Produktet baserer seg på standardiserte protokoller og tjenester for å levere føderert identitet.
Formålet med regional autentiseringstjeneste er å tilby en autentiseringstjeneste som kan benyttes av tjenester/systemer som støtter føderert autentisering.
En tjeneste som bruker regional autentiseringstjeneste for autentisering i samsvar med nivået som er angitt i kapittel 3.3, vil automatisk oppfylle denne policyen.

3.1 Definisjon av sikkerhetsnivåer innen autentisering

eIDAS (Electronic Identification, Authentication and Trust Services) er en EU-forordning som har til hensikt å styrke og harmonisere elektronisk identifisering (eID) og tillitstjenester innen det digitale indre markedet i EU. Dette inkluderer autentisering, signaturer og dokumentintegritet. eIDAS-forordningen definerer tre sikkerhetsnivåer for autentisering.

1. **Lav** - Det laveste sikkerhetsnivået er designet for situasjoner med begrenset risiko for misbruk eller konsekvenser ved feilaktig identifisering. Autentiseringsprosessen på dette nivået kan innebære enkel brukernavn/passord-kombinasjon eller andre enkle mekanismer for å bevise identitet.

2. **Betydelig** - Det mellomste sikkerhetsnivået er ment for situasjoner med moderat risiko for misbruk og konsekvenser ved feilaktig identifisering. Autentisering på dette nivået krever tofaktorautentisering.

3. **Høy** – Det høyeste sikkerhetsnivået har flere faktorer for autentisering, inkludert kryptografiske teknikker, sertifiseringsinstanser (CA) som utsteder kvalifiserte sertifikater for elektroniske signaturer og segl, samt bruk av FIDO2-protokollen for sterk, passordløs autentisering.

3.2 Autentiseringsmetoder og sikkerhetsnivå Helse Sør-Øst

Helse Sør-Øst har et sett med internt godkjente autentiseringsmetoder som kan brukes for å få tilgang til informasjonssystemer. En autentiseringsmetode kan ha en eller to faktorer og er definert på et av sikkerhetsnivåene som benyttes i Norge og innen EU. eIDAS-forordningen stiller krav til disse og tilsynsmyndigheten i Norge (NKOM) sikrer kvaliteten på metodene.

Følgende autentiseringsmetoder er tillatt i Helse Sør-Øst: Er autentiseringsmetoden godkjent av NKOM? Se **ja/nei** i parentes		
Høy	**Betydelig**	**Lav**
Buypass ID på smartkort (**Ja**)	*Per i dag finnes det ingen autentiseringsmetoder på nivå betydelig som er godkjent av NKOM.*	Brukernavn og passord mot AD (**Nei**)
Buypass ID på mobil (**Ja**)		Mobilbasert MFA (**Nei**) Cisco Duo, SecurEnvoy, MS Authenticator Merk: SMS er ikke godkjent autentiseringsmetode
Buypass ID med FIDO2 (**Ja**)		Buypass PKI med lokal autoritet (kun AHUS) (**Nei**)
Bank ID (**Ja**)		Windows Hello (**Nei**)
		Microsofts FIDO2-løsning og andre tilsvarende løsninger som ikke har NKOMs godkjenning (**Nei**)

3.3 Scenarier og krav til sikkerhetsnivå

Valg av autentiseringsmetode for et gitt brukerscenario i en tjeneste er basert på flere faktorer:

- Brukergruppe
- Lokasjon
- Utstyr/enhet
- Juridisk perspektiv
- Brukerperspektiv

Tabellen under inneholder de vanligste scenariene og identifisert sikkerhetsnivå på autentiseringsmetoden som benyttes. En bruker kan selv velge metode på et gitt sikkerhetsnivå dersom det er flere alternativer i listen over godkjente autentiseringsmetoder.

Område	Scenario	Sikkerhetsnivå
Arbeidsflate	PC-login, laptop/stasjonær/tynnklient	Betydelig
Arbeidsflate	Admin desktop, tilgang til arbeidsflate for administrative tjenester	Høy
Mobil	Mobil funksjonsenhet: Tilgang til sensitive personopplysninger utenfor helseforetaket	Høy
Mobil	Mobil, personlig enhet: Tilgang på administrative verktøy som e-post, kalender og møtenotater	Betydelig
Mobil	Mobil delt enhet: Gir tilgang til sensitive personopplysninger på mobile enheter lokalisert på et helseforetak	Høy
Mobil	Mobil funksjonsenhet som er lokalisert i ambulanse eller ambulansehelikopter	Høy
Lokal tilgang	Tilgang til klinisk fagapplikasjon	Høy
Lokal tilgang	Tilgang til virksomhetssensitiv/virksomhetskritisk informasjon	Høy
Lokal tilgang	Tilgang til detaljert informasjon på storskjerm: Gir tilgang til sensitive personopplysninger	Høy
Fjernaksess	Ekstern desktop; Tilgang til arbeidsflate og privilegert tilgangsportal for leverandør på ekstern lokasjon	Betydelig
Fjernaksess	Tilgang til arbeidsflate for ansatt og innleid fra ekstern lokasjon (VPN)	Høy
Privilegert tilgang	Tilgang til privilegert arbeidsflate/server	Høy

4. Krav til passord for helseforetakene i Helse Sør-Øst

Helseforetakene i Helse Sør-Øst har kommet til enighet om følgende regionale passordkrav:

Den ansattes plikter	Regionale krav til passord for helseforetakene i Helse Sør-Øst
- Passordet er personlig og skal aldri deles - Passordet skal aldri skrives ned - Ved mistanke om tap av passordkonfidensialitet, skal brukerservice umiddelbart kontaktes og passord skal endres - Passordet skal ikke benyttes på andre tjenester (for eksempel privat e-post, Facebook eller lignende)	- Alle brukerkontoer skal ha passord - Passordet skal bestå av minst åtte tegn[1] - Passordet skal ha minst 3 av 5 følgende egenskaper: - *Store bokstaver (A-Z)* - *Små bokstaver (a-z)* - *Tall (0-9)* - *Spesialtegn (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)* - *Unicode* - Passord må byttes hver 90. dag. - Ansatte kan alternativt velge passord uten foreldelse («password never expires») og kompleksitetskrav ved å benytte passord som er 16 tegn eller lengre. Dette kan bestilles som valg i BAT / Min Sykehuspartner HF - Tofaktorløsninger som smartkort eller tilsvarende kan ha kortere og enklere passord/PIN-koder.[2] - Brukerkonto stenges etter 10 sammenhengende mislykkede påloggingsforsøk innen 15 minutters tid - Brukerkontoer kan åpnes automatisk etter tidligst 15 minutter - Passordet må være forskjellig fra tidligere passord, systemet skal huske de siste 13 passordene - Påloggінger, inkludert forsøk på feilaktig pålogging, skal logges og spores tilbake til minimum en maskinadresse

[1] Policyen bygger på god praksis, jf. NIST SP 800-63b pkt 5.1.1.1, jf. Appendix A (2017, oppdatert 2020); Anbefalinger fra NCSC (2018); Password policy recommendations - Microsoft 365 admin | Microsoft Docs (2021)

[2] Tidligere unntak for smartkortløsning som AHUS benytter dekkes av dette punktet.

4.1 Krav til PIN-kode for pålogging for helseforetakene i Helse Sør-Øst

PIN-koder som benyttes til pålogging har følgende krav

Den ansattes plikter	Regionale krav til PIN-kode for helseforetakene i Helse Sør-Øst
- PIN-kode er personlig og skal aldri deles - PIN-kode skal aldri skrives ned - PIN-kode skal være vanskelig å gjette - Ved mistanke om tap av PIN-konfidensialitet, skal passord endres umiddelbart og ny PIN opprettes	- PIN-kode skal bestå av minst 4 numeriske tegn - Unngå tallserier, like påfølgende tall og lett gjenkjennelige tall slik som f.eks. fødselsdato

5. Unntak fra passordkrav for eldre informasjonssystemer

Flere av helseforetakene har eldre systemer eller andre typer systemer som teknisk ikke kan etterleve regionale krav for passordkompleksitet. Hvert helseforetak er ansvarlig for å utarbeide en tilfredsstillende passordsikkerhet for disse systemene.

Helseforetak anbefales ved anskaffelse av nye, eller oppdatering av eksisterende, informasjonssystemer at det kravstilles at informasjonssystemet støtter Regional Autentiseringspolicy, eller at informasjonssystemet kan integreres med sentral autentiseringsløsning (AD).

6. Administratorpassord i Helse Sør-Øst

Sykehuspartner HF har besluttet følgende passordkrav hvor det benyttes administratorrettigheter.

6.1 Personlige administratorpassord

Følgende krav gjelder for personlige administratorpassord:

Den ansattes plikter	Regionale krav til passord for helseforetakene i Helse Sør-Øst
- Passordet er personlig og skal aldri deles - Passordet skal aldri skrives ned - Ved mistanke om tap av passordkonfidensialitet, skal brukerservice umiddelbart kontaktes og passord skal endres, og seksjon sikkerhet skal varsles - Passordet skal ikke benyttes på andre tjenester (for eksempel privat e-post, Facebook eller lignende) - Passordet skal være vanskelig å gjette	- Alle administratorkontoer skal ha passord - Passordet skal bestå av minst 16 tegn[3] - Passordet skal ha minst 3 av 5 følgende egenskaper: - *Store bokstaver (A-Z)* - *Små bokstaver (a-z)* - *Tall (0-9)* - *Spesialtegn (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)* - *Unicode* - Passordet må endres minst hver 90. dag, «password never expires» eller tilsvarende attributter skal ikke aktiveres - Brukerkonto stenges etter 10 sammenhengende mislykkede påloggingsforsøk innen 15 minutters tid - Brukerkontoer kan åpnes automatisk etter tidligst 15 min - Passordet må være forskjellig fra tidligere passord, systemet skal huske de siste 13 passordene - Påloggінger, inkludert forsøk på feilaktig pålogging, skal logges og spores tilbake til minimum en maskinadresse - Tofaktorautentisering er påkrevd - Det skal etableres utvidet logging hvem som logger på og hvilke handlinger som utføres - Logger skal gå inn i sentralt loggmottak for å bevare integritet

[3] Anbefalingen bygger her på Passordanbefalinger fra Nasjonal sikkerhetsmyndighet (NSM) fra 2018

6.2 Upersonlige administratorpassord

Upersonlige administratorpassord («konsollpassord») er kontoer som ikke er knyttet til en person, f.eks. servicekontoer, «root», «db_admin» mv. Disse skal ordinært sett ikke benyttes, og tilgang til dem skal begrenses. I motsetning til personlige administratorpassord autentiseres det direkte mot systemet, ikke katalogtjenesten. Følgende krav gjelder for konsollpassord:

Den ansattes plikter	**Regionale krav til passord for helseforetakene i Helse Sør-Øst**

- Passordet skal aldri lagres utenfor godkjent passordsystem
- Ved mistanke om tap av passordkonfidensialitet, skal passordet umiddelbart endres og seksjon sikkerhet skal varsles
- Passordet skal ikke benyttes på andre tjenester (for eksempel privat e-post, Facebook eller lignende)
- Passordet skal være unikt for det enkelte systemet
	- Passord skal kun oppbevares i sikkert, digitalt passordhvelv.
	- Passordet skal bestå av minst 16 tegn
	- Passordet skal ha minst 3 av 5 følgende egenskaper:
	  - *Store bokstaver (A-Z)*
	  - *Små bokstaver (a-z)*
	  - *Tall (0-9)*
	  - *Spesialtegn (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)*
	  - *Unicode*
	- All bruk av konsollpassord i produksjonssystemer skal registreres / loggføres
	- Påloggінger, inkludert forsøk på feilaktig pålogging, skal logges og spores tilbake til minimum en maskinadresse
	- Det skal etableres utvidet logging hvem som logger på og hvilke handlinger som utføres
	- Logger skal gå inn i sentralt loggmottak for å bevare integritet

7. Digitalt passordhvelv og fysisk passordsafe

Sykehuspartner har etablert digitale og fysiske tiltak for å sikre bl.a. passord, kryptografiske nøkler og lignende. Passord til systemer som ikke er tilknyttet sentral autentiseringstjeneste (AD eller lignende) skal oppbevares i denne løsningen.

Passordsafe skal understøtte virksomhetens mål for tilgangsstyring:

- Begrenset levetid for administratorbrukere
- Tilganger, også for administratorbrukere, skal sperres uten ugrunnet opphold

- Administrator skal ikke ha permanent kjennskap til ikke-individuelle passord

Det er linjeledere i Sykehuspartner som er ansvarlig for at passordhvelv benyttes for eget fagområde. Linjeleder vil være ansvarlig for at det flyttes passord fra digitalt passordhvelv til fysisk passordsafe, jfr. egne rutiner for dette.

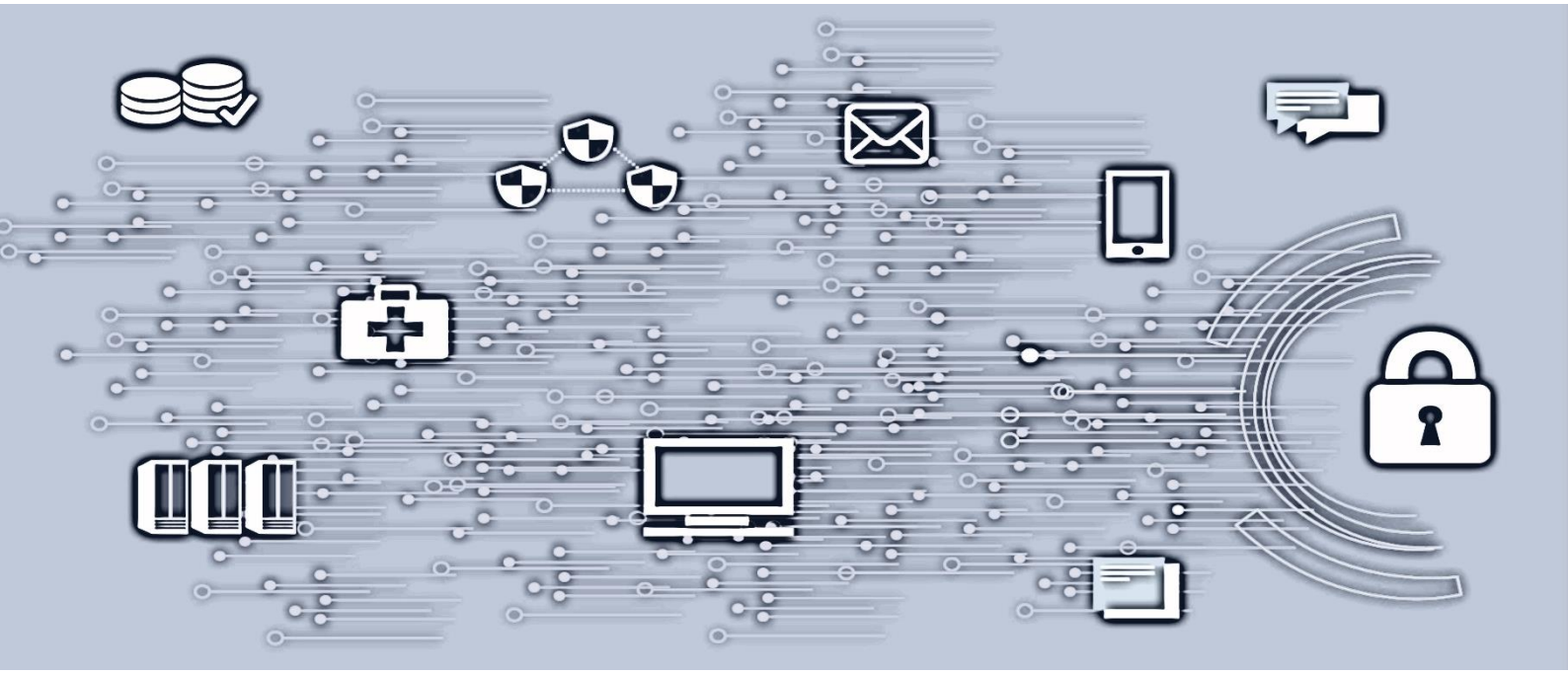
8. Avvik

Avvik fra denne policyen som ikke er adressert i ROS-prosessen (risiko- og sårbarhetsanalyse) skal rapporteres gjennom foretakets avvikshåndteringssystem.

Et avvik i denne policyen refererer til enhver handling, hendelse eller tilstand som avviker fra de fastsatte kravene eller prosedyrene, spesielt med hensyn til autentiseringsmetoder og passordkrav. Dette kan inkludere, men er ikke begrenset til, bruk av ikke-godkjente autentiseringsmetoder eller opprettelse av passord som ikke oppfyller de definerte kravene.

SYKEHUSPARTNER

Regionale sikkerhetsprinsipper og – krav for skytjenester



Innhold

Versjon	Dato	Godkjent av
1.0	26.03.2021	Christian Jacobsen
1.1	23.03.2022	Christian Jacobsen
1.2	01.09.2023	Informasjonssikkerhetsleder

1. Introduksjon

Grunnmur for skytjenester skal understøtte tjenester som etableres i skyen uansett tjeneste- og leveransemodell. Dette dokumentet er en del av sikkerhetsarkitekturen «Grunnmur for skytjenester». Dokumentene som utgjør «Grunnmur for skytjenester» utgjør et sett med basiskapabiliteter og sikkerhetsprinsipper som beskriver informasjonssikkerhet og personvernstiltak for hvordan skytjenester tas i bruk, inkludert bla. tilgangsstyring, risikostyring, leverandørhåndtering, sikkerhetskrav, personvern og endring- og hendelseshåndtering. Dokumentene er en del av Sykehuspartner HF sitt ledelsessystem for informasjonssikkerhet (ISMS).

2 Formål

Regionale sikkerhetsprinsipper og -krav for skytjenester er et dokument som beskriver og stiller detaljerte krav i forbindelse med konsum av skytjenester. Kravene og prinsippene i dette dokumentet kan direkte spores tilbake til overordnede krav, forretningsbehov og drivere for sikkerhet i Regional sikkerhetspolicy for skytjenester, og begge dokumentene må leses i sammenheng. Kravene som fremkommer i dette dokumentet, må sees på som anbefalinger og kan benyttes for å utvikle en kravspesifikasjon for skytjenester.

2.1 Målgruppe

Sikkerhetsprinsippene skal detaljere kapitlene fra «Regional sikkerhetspolicy for skytjenester». Dokumentet er rettet mot flere målgrupper, blant annet;

- Prosjekter som skal benytte skytjenester i sine leveranser
- Anskaffelsesprosesser som involverer skytjenester
- Tjenestedesignere, løsningsdesignere og arkitekter
- Juridisk
- Personvern
- Risiko- og sårbarhetsrådgivere som skal utføre ROS av skytjenester
- Sikkerhetsressurser som arbeider med operativ- eller strategisk sikkerhet
- Internrevisjon/Sikkerhetsrevisjon
- Leverandøroppfølging og kontraktstyring

2.2 Virkeområde

Dokumentet gjelder for de leveranser eller tjenester som på en eller annen måte omfatter bruk av skytjenester i Helse Sør-Øst.

2.3 Avhengigheter og forutsetninger

I de tilfeller dette dokumentet påpeker manglende dokumentasjon i regionen, må dette utarbeides for å dekke de mangler som fremkommer.

3 Kilder

Se kildehenvisninger i Regional Sikkerhetspolicy for skytjenester kapittel 3.

4 Forkortelser og begreper

Forkortelse/begrep	Fullt navn/forklaring
ASR	Arkitektur i program og prosjekter
BCP	Business Continuity Plans / (forretnings)kontinuitetsplaner, ofte en del av et selskaps beredskapsplaner
BYOK	Bring Your Own Key
BYOE	Bring Your Own Encryption
CAIQ	Consensus Assessment Initiative Questionaire er et regneark som kan lastes ned fra CSA sine hjemmesider. Skjemaet inneholder en rekke ja/nei-spørsmål som overlapper de ulike kontrollene i Cloud Control Matrix (CCM)
CASB	Cloud Access Security Broker
CCM	Cloud Control Matrix er en liste med beste praksiser knyttet til skyløsninger og kommer fra Cloud Security Alliance (CSA) sine sikkerhetsveiledninger for databehandlinger i skyen.
CERT	Computer Emergency Response Team
Community cloud	Skytjenester for fellesskap av virksomheter
CSA	Cloud Security Alliance
CSP	Cloud Service Provider (se skyleverandør)
DBA	Databehandleravtale
DevOps	Software Development and Information Technology Operations
DFØ	Direktoratet for forvaltning og økonomistyring
DLP	Data Loss Prevention
DPIA	Data Protection Impact Assessment, Personvernkonsekvensvurdering
DRP	Disaster Recovery Plans / krisegjenopprettingsplaner, ofte en del av et selskaps beredskapsplaner
eIDAS	Electronic Identification, Authentication and Trust Services. EU regulativ om elektronisk ID.
EMM	Enterprise Mobility Management
GDPR	General Data Protection Regulation (Personvernforordningen)
HF	Helseforetakene under Helse Sør-Øst inkludert Sykehuspartner
Helseforetakene i regionen	Her menes alle HF, inkludert Sykehuspartner HF og Helse Sør-Øst RHF.
HSØ	Helse Sør-Øst RHF
Hybrid cloud	Kombinasjon av private og public cloud. Både eksklusive og delte skytjenester
IaaS	Infrastructure-as-a-Service
IAM	Identity and Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMB	Information Security Management Board. Organ som skal sørge for helhetlig sikkerhetsledelse i Sykehuspartner HF
ISMS	Information Security Management System
Leveransemodell sky	Typen leveranse av sky: private/public/hybrid/community cloud I henhold til Normen og NIST sin definisjon.
LG1	Ledermøtet SPHF
MAM	Mobile Application Management
MDM	Mobile Device Management

MFA	Multi Factor Authentication
NDA	Non-Disclosure Agreement
NKOM	Nasjonal kommunikasjonsmyndighet
NSM	Nasjonal Sikkerhetsmyndighet
On-Premise Private Cloud	Infrastrukturen er tilbudt eksklusivt for en virksomhet, på et lokalt eid, kontrollert og driftet datasenter.
PaaS	Platform-as-a-Service
PKI	Public Key Infrastructure
PKV	Personvernkonsekvensvurdering (DPIA)
Private cloud	Infrastrukturen er tilbudt eksklusivt for en virksomhet. Den kan være eiet, kontrollert og driftet av virksomheten (og være i eget datasenter som tar i bruk prinsippene for skytjenester), en tredjepart, eller en kombinasjon av disse.
Public cloud	Infrastrukturen er tilbudt for åpen bruk for alle virksomheter og privatpersoner. Den kan være eiet, håndtert og operert av en kommersiell, akademisk, ideell eller offentlig organisasjon eller en kombinasjon av slike.
RPO	Recovery Point Objective – Største akseptable datatap målt i tid, gir rammer for hvor ofte back-up skal tas.
RTO	Recovery Time Objective – Lengste akseptable nedetid i strekk, setter ambisjonsnivå for hvor fort tjenesten skal kunne gjenopprettes ved en feilsituasjon eller hendelse.
RSR	Regionalt Sikkerhetsfaglig Råd
RSS	Regional Sikkerhetspolicy for Skytjenester
RSPS	Regionale Sikkerhetsprinsipper og -krav for Skytjenester
RSV	Regionalt Sikkerhetsvurderings team
Regionen	Helse Sør-Øst med underliggende HF
SaaS	Software-as-a-Service
SABSA	Sherwood Applied Business Security Architecture
SECaaS	Security-as-a-Service
Skyleverandør	En skyleverandør tilbyr skybasert plattform, infrastruktur, program eller lagringstjenester
Skytjeneste	Skytjenester er en samlebetegnelse for leveransemodeller som muliggjør tilgjengelige, tilpassede, «on-demand», tilgang til en pool med delte ressurser som kan skaleres opp eller ned (både for kunde og leverandør). Infrastrukturen som leverer skytjenesten kan være tilgjengelig både i egen infrastruktur, og via eksterne nettverk (utenfor virksomhetens infrastruktur).
SLA	Service Level Agreement
SPARK	Sykehuspartner Arkitekturråd
SPHF	Sykehuspartner HF
TCO	Total Cost of Ownership
Tjenestemodell sky	Typen skytjeneste: IaaS, PaaS, SaaS
TOGAF	Arkitektur-rammeverk

5 SABSA rammeverk for sikkerhetsarkitektur

SABSA-rammeverket lagt til grunn for sikkerhetsarkitekturen som understøtter RSPS. Dette er nærmere omtalt i kapittel 5 i Regional Sikkerhetspolicy for skytjenester (RSS).

6 Kontekstuell arkitektur

Se beskrivelsen av kontekstuell arkitektur i Regional Sikkerhetspolicy for skytjenester.

7 Sikkerhetsprinsipper og -krav for skytjenester

I det følgende hovedkapittelet finner du sikkerhetsprinsippene for bruk av skytjenester. Prinsippene er delt inn etter kapitlene i Regional Sikkerhetspolicy for skytjenester, slik at du enkelt kan finne korresponderende kapittel i RSS mot prinsippet i RSPS.

Sikkerhetsprinsipper og -krav for skytjenester, Sikkerhetspolicy for skytjenester og skyleverandørens besvarelse av CAIQ utgjør samlet den sikkerhetsmessige dokumentasjonen som må utarbeides for tjenesten, og er i sin tur gjenstand for Risiko- og sårbarhetsvurdering etter gjeldende prosess i SPHF.

Sikkerhetsprinsipper og -krav for skytjenester er godt egnet til å legges til grunn for en kravspesifikasjon knyttet til anskaffelser.

Unntak fra sikkerhetsprinsippene skal dokumenteres. Grunnlaget for å beslutte unntak skal dokumenteres i form av risikovurdering.

Hvert prinsipp er delt opp i ett eller flere hovedprinsipp. Hvert hovedprinsipp har tilhørende delprinsipper som utdyper og detaljerer dets respektive hovedprinsipp. Alle hovedprinsipp gjengir hvilken forretningsdriver (BD – Business Driver) i RSS den gjenspeiler og hovedprinsippets kildegrunnlag. Delprinsippene er på sin side knyttet opp mot hovedkontrollene i CSA CAIQ (Control ID) der hvor dette er relevant.

Det bemerkes at prinsippene ikke er uttømmende, og du kan måtte se til andre kilder internt eller eksternt for å komplettere din skyleveranse. Dette gjelder særlig i de tilfeller hvor man har tjenestespesifikke sikkerhetskrav, eksempelvis knyttet til

- Behandlingsrettede helseregistre (egne krav til sporbarhet, logging og sperring osv. ref. NO-19 i ISMS).
- Bokføringslovgivning
- Oppbevaring over tid (Arkivlovgivning)

Ved behov for tilgang til Sykehuspartner-interne dokumenter som det henvises til i disse sikkerhetsprinsippene og –kravene, så kan helseforetakene rette en henvendelse til Avdeling Sikkerhet i SPHF for å få utlevert en kopi. Øvrige interessenter må rette en formell innsynsforespørsel iht. Offentleglovas bestemmelser.

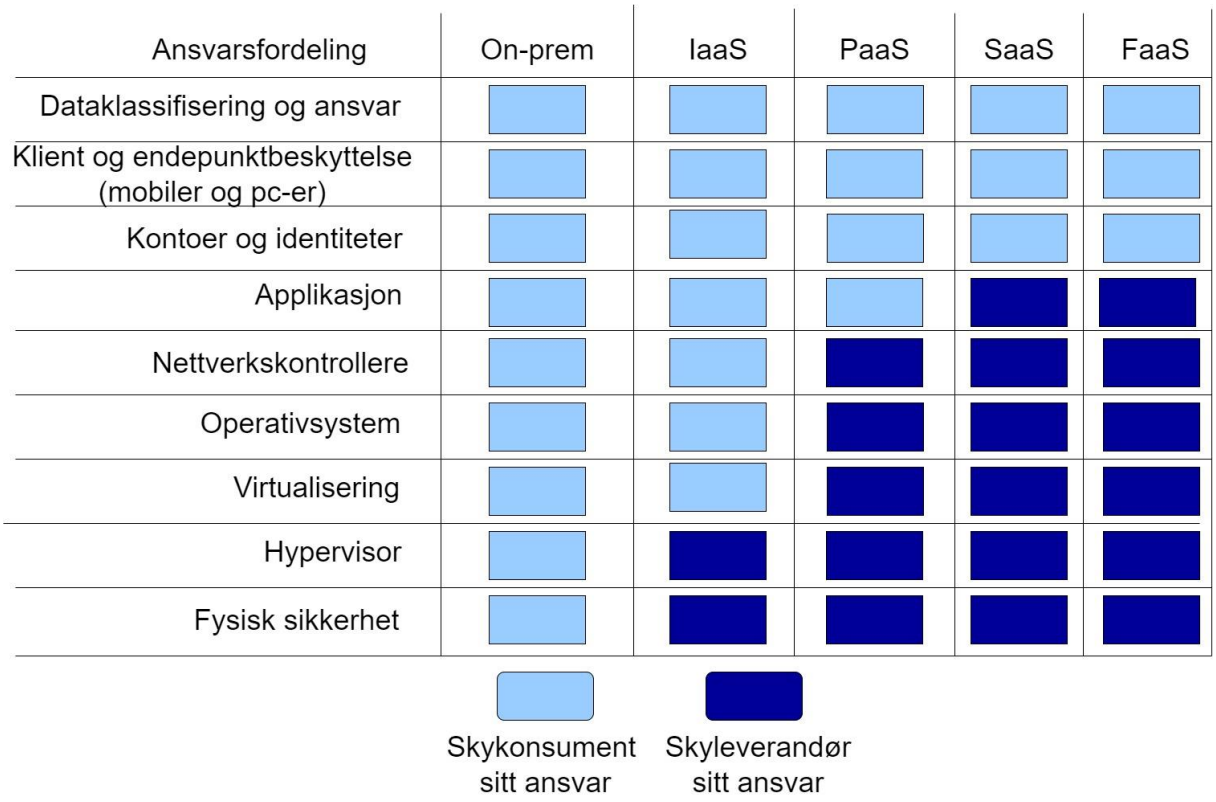
7.1 Sikkerhetsledelse og ansvar

Behandlingsansvarlig bestemmer formålet til personopplysningene. Hvem som er behandlingsansvarlig vil variere fra tjeneste til tjeneste. Dette betyr at ansvaret for å etterleve regelverk ikke kan fraskrives behandlingsansvarlig, selv om dataene behandles hos en skyleverandør. SPHF er databehandler for de øvrige HF-ene, og skal forvalte IKT-avtaler i regionen på vegne av HF-ene.

#	Hovedprinsipp	Business Driver	Kilde
7.1.a	Dataansvarlig er hovedansvarlig for at data som blir behandlet i sky, etterlever gjeldende regelverk.	BD7	RSS Normen GDPR art. 5
#	**Delprinsipp**		**CAIQ Control ID**
7.1.a.1	Dataansvarlig skal dokumentere hjemmelsgrunnlag for behandling av data i sky. Hjemmelsgrunnlag må dokumenteres per tjeneste.		N/A
7.1.a.2	Dataansvarlig har ansvar for at data som lagres i sky er klassifisert i henhold til gjeldende modell for informasjonsklassifisering og ihht krav i kapittel 7.6 Dataklassifisering i dette dokumentet.		N/A
7.1.a.3	SPHF skal sørge for at data håndteres i henhold til klassifisering gjennom organisatoriske og tekniske tiltak og avtaler med leverandør.		DSP-01.1 DSP-012.1 CEK-04.1

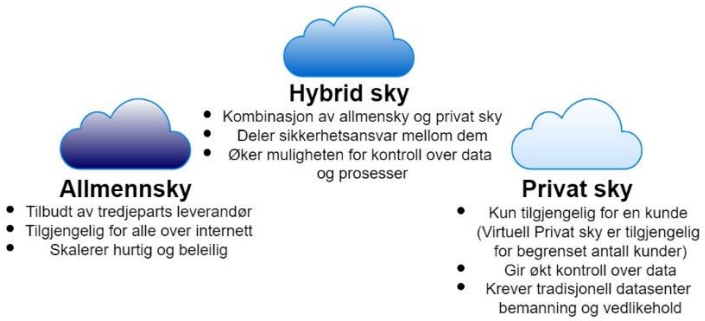
7.1.1 Ansvarsfordeling for sikkerhetstiltak

#	Hovedprinsipp	Business Driver	Kilde
7.1.1.a	Sikringstiltak av skytjenester skal utføres med hensyn til valgt tjeneste- og leveransemodell. Tjenestemodeller: IaaS, PaaS, FaaS, SaaS. Leveransemodeller: Privat, Offentlig/allmenn, Hybrid.	BD7	Difi rapport 2018:6 Normen
#	**Delprinsipp**		**CAIQ Control ID**
7.1.1.a.1	Ansvaret for sikringstiltak av skytjenester skal spesifiseres i kontrakt med skyleverandør.		STA-02.1 STA-04.1 STA-09.1



Figur 3 – Matrise for sikkerhetstiltak mellom ulike typer tjenestemodeller

Ansvarsfordeling i skytjenester viser hvem som har ansvar for hvilke deler av skyen. I en SaaS vil det meste av ansvaret for tjenesten ligge hos skyleverandør, mens i en IaaS vil kunden ha ansvar operativsystem, virtuelle maskiner og det virtuelle nettverket. Dette gjelder alt fra utvikling til sikkerhet på områdene. Ansvaret kan også ligge delt mellom kunde og skyleverandør. I tillegg til ansvarsmatrise finnes det forskjellige leveransemodeller; privat, offentlig/allmenn og hybrid sky. Offentlig sky tilbys av tredjepart hvor det er ingen begrensning for hvem som har mulighet til å leie tjenester av tilbyder. Privat sky er en sky som kun benyttes av en kunde, og vil ikke dele ressurser med andre. Hybrid sky er forskjellige skytjenester som en bundet sammen. Hvis en har en privat sky hos skyleverandør 1 og offentlig sky hos skyleverandør 2 vil dette til sammen være en hybrid skyløsning.



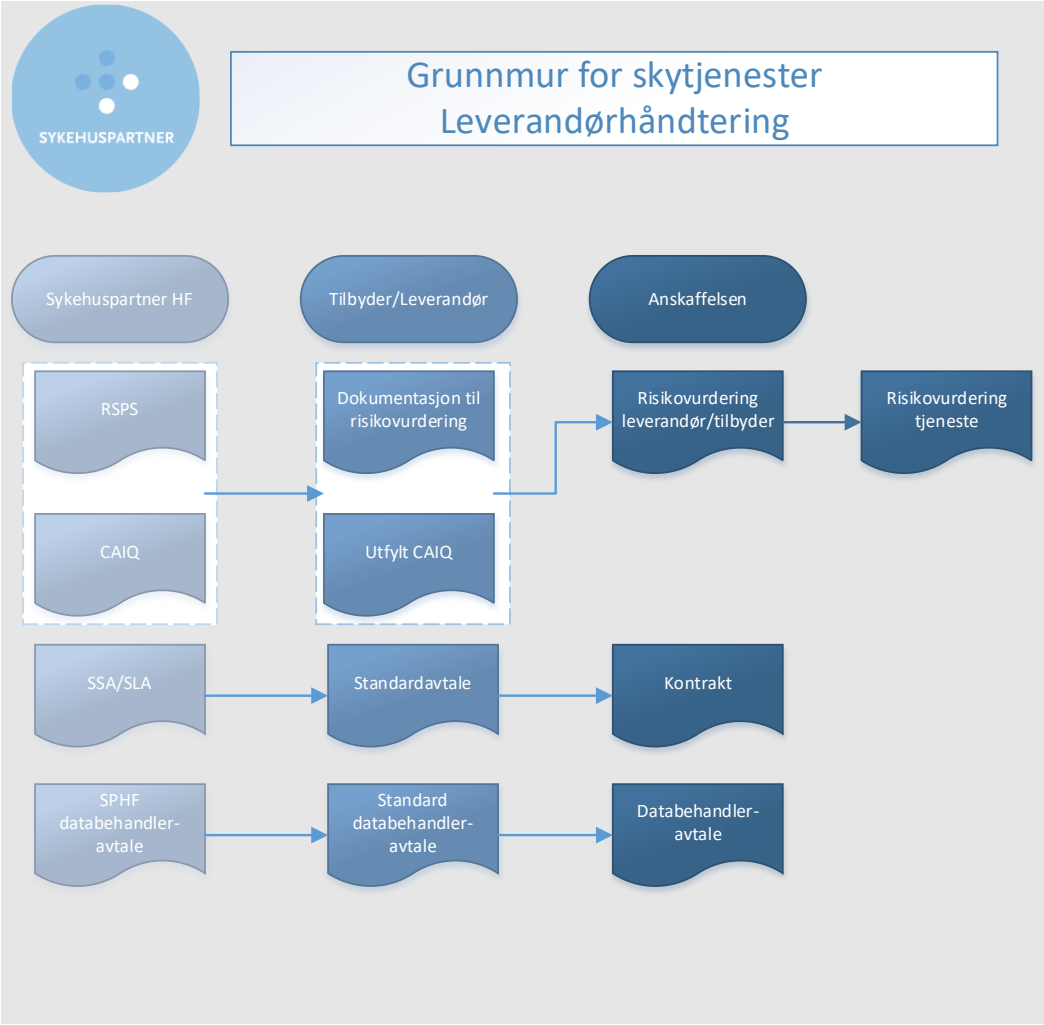
7.1.2 Intern forvaltning og kompetanse

#	Hovedprinsipp	Business Driver	Kilde
7.1.2.a	SPHF skal sørge for tilgjengelig og relevant kompetanse til å forvalte sine ansvarsområder ved bruk av skytjenester.	BD7	RSS
#	Delprinsipp		CAIQ Control ID
7.1.2.a.1	Det skal være allokert relevante ressurser slik at leverandøren og tjenesten kan følges opp på en forsvarlig måte.		N/A
7.1.2.a.2	Det skal gjennomføres opplæring i policy og prosedyrer som er relevant for alle roller i systemet. Dette innbefatter samtlige brukere og administratorer av systemet, samt eventuelle kontraktører og tredjepartsbrukere.		HRS-11.1 HRS-12.2

7.2 Leverandørhåndtering

Dette kapittelet omhandler hvordan SPHF skal håndtere eksisterende og potensielle leverandører både før, under og etter at en anskaffelse gjøres. Etter en gjennomgang av prinsippene i de underliggende delkapitlene samt tilbyders besvarelse av CAIQ, vil resultatet være tre produkter for å bistå med en helhetlig oversikt over leverandørhåndtering av skytjenester.

- Risikovurdering og eventuelle landvurderinger knyttet til valgt løsning
- Tjenesteleveranseavtale (SLA)
- Databehandleravtale der leverandøren håndterer personopplysninger



7.2.1 Risikovurdering av leverandører

Denne seksjonen handler om risikovurdering av leverandører. Risikovurdering av de enkelte tjenestene omhandles i kapittel 7.3 Risikostyring/risikovurdering.

#	Hovedprinsipp	Business Driver	Kilde
7.2.1.a	Det skal gjøres en modenhetsvurdering av leverandør før en eventuell avtale inngås. CAIQ og RSPS vil benyttes som underlag for denne vurderingen. Det skal gjøres innledende risikovurdering av leverandøren før en eventuell avtale inngås basert på leverandørens svar på sikkerhetskrav i konkurransegrunnlaget.	BD12	ISMS RSS
#	Delprinsipp		CAIQ Control ID
7.2.1.a.1	Tilbyders utfylte CAIQ skal være underlag i risikovurderingen av leverandøren. Tilbyders CAIQ kan gjerne være basert på underleverandørs/skyleverandørens CAIQ, der det er relevant,		N/A

	for å sikre en god besvarelse som adresseres relevante forhold i tjenesten.		
7.2.1.a.2	Alle leverandører og underleverandører som skal behandle personopplysninger skal kunne dokumentere egen sikring av personopplysninger iht. ISO 27001, 27017, 27018 eller tilsvarende.		STA-12.1 GRC-05.1
#	Hovedprinsipp	Business Driver	Kilde
7.2.1.b	Ved vesentlige endringer i skyleverandørens standardvilkår skal leverandøren varsle Sykehuspartner slik at Sykehuspartner kan ta stilling til endringen.	BD12	RSS

7.2.2 Avtaler og kontrakter

#	Hovedprinsipp	Business Driver	Kilde
7.2.2.a	Tjenesteutsetting i form av skytjenester skal kontraktsfestes mellom partene, og foreligge før skytjenesten tas i bruk.	BD8, BD12	RSS Normen kapittel 5.7
#	Delprinsipp		CAIQ Control ID
7.2.2.a.1	SPHF skal så langt det er mulig søke å inngå avtale basert på Statens Standardavtaler (SSA).		N/A
7.2.2.a.2	I de tilfeller der kontraktspart stiller med sin standardavtale må det sikres at denne avtalen ivaretar relevante regulatoriske krav og sikkerhetsprinsipper. Eventuelle avvik fra standardavtale fra kontraktspart, skal inntas i tjenestens risiko- og sårbarhetsvurdering.		A&A-04.1
7.2.2.a.3	Krav til revisjon for den enkelte tjeneste skal fremkomme av avtaleverket mellom SPHF og skyleverandør. Se også kapittel 7.5 Revisjon.		A&A-01.1

#	Hovedprinsipp	Business Driver	Kilde
7.2.2.b	Leverandøren skal til enhver tid ha oversikt over alle aktuelle underleverandører i leverandørkjeden. Leverandøren skal på oppfordring fra SPHF kunne presentere en oversikt over alle underleverandører og tjenester disse yter for aktuell avtale.	BD8, BD12	RSS
#	Delprinsipp		CAIQ Control ID
7.2.2.b.1	Leverandøren skal føre en oversikt (protokoll) over alle kategorier av behandlingsaktiviteter som utføres på vegne av databehandler/dataansvarlig.		
7.2.2.b.2	Databehandleravtale skal være signert før behandling av personopplysninger kan skje.		

7.2.3 Tjenesteleveranseavtaler (SLA)

#	Hovedprinsipp	Business Driver	Kilde
7.2.3.a	Tjenestene som skal leveres av leverandøren skal formaliseres i SLA-avtaler, og inkludere sikkerhetskrav samt ansvar for risiko.	BD12	RSS
#	Delprinsipp		CAIQ Control ID
7.2.3.a.1	SLA avtalen skal reflektere de krav som er relevante for tjenesten. Kravene skal være konkrete og målbare. Eksempelvis: • Oppetid, • Svartid på henvendelser, • Brukeropplevd treghet, mv.		BCR-01
7.2.3.a.2	Avtalen skal inneholde en plan for ivaretakelse av informasjonssikkerhet og personvern ved avslutning av skytjenesten (exit strategi).		IPY-04.1

7.2.4 Databehandling og databehandleravtaler

#	Hovedprinsipp	Business Driver	Kilde
7.2.4.a	Ved behandling av personopplysninger hos skyleverandøren skal det inngås en databehandleravtale før tjenesten tas i bruk.	BD4, BD12	RSS Datatilsynet
#	Delprinsipp		CAIQ Control ID
7.2.4.a.1	Sykehuspartner skal, som avtaleforvalter i regionen, tilstrebe å inngå databehandleravtale med skyleverandør, på HSØ-malverk. Ved bruk av skyleverandørens databehandleravtale skal denne kvalitetssikres av Juridisk avdeling før den tas i bruk.		N/A
7.2.4.a.2	Databehandlers forpliktelser skal kontraktuelt og i praksis videreføres med samme vilkår til eventuelle underdatabehandlere. Dette er det databehandlers ansvar å påse.		STA-12
7.2.4.a.3	Formålet med behandling av personopplysninger skal fremkomme av databehandleravtalen.		N/A
7.2.4.a.4	Ved behandling av personopplysninger skal Regional Protokoll over Behandlingsaktiviteter fylles ut og holdes oppdatert.		N/A

7.3 Risikostyring/risikovurdering

Denne seksjonen handler om risikovurdering av levert tjeneste.

#	Hovedprinsipp	Business Driver	Kilde
7.3.a	Skytjenesten skal risiko- og sårbarhetsvurderes i henhold til SPHFs risikovurderingsmetodikk og etter gjeldende prosess og malverk.	BD1, BD12	ISMS RSS
#	Delprinsipp		CAIQ Control ID
7.3.a.1	CAIQ og løsningsdesign skal inngå som underlag til risikovurderingen.		N/A
7.3.a.2	Risikovurdering skal gjennomføres ved alle endringer som kan ha betydning for informasjonssikkerheten.		BCR-02
7.3.a.3	Risikovurderingen skal inkludere en landvurdering der dette er relevant (som regel 3. parts land utenfor EU/EØS). Ved skytjenester i tredjeland må ytterlige vurderinger gjøres i henhold til dagens situasjon.		BCR-02

7.4 Personvern

Helse- og personopplysninger i skyen skal behandles i tråd med gjeldende lovkrav og øvrig styrende dokumentasjon i Helse Sør-Øst. SPHF og leverandører vil ha rollen som databehandlere og vil ha selvstendige plikter etter personvernlovgivningen, som blant annet å følge personvernprinsippene i GDPR artikkel 5. SPHF og leverandører skal kun behandle personopplysninger etter instruks fra dataansvarlig.

Se til SPHFs interne sider for personvern for ytterligere informasjon om temaet.

#	Hovedprinsipp	Business Driver	Kilde
7.4.a	All behandling av personopplysninger må ha et rettslig grunnlag for å være lovlig. SPHF og leverandør, som databehandler, har et selvstendig ansvar for å følge lovgivning og skal kun behandle personopplysninger på instruks fra dataansvarlig.	BD1 BD4	RSS GDPR art. 6 Normen kapittel 4.1
#	Delprinsipp		CAIQ Control ID
7.4.a.1	Ved bruk av skytjenester skal det være rettslig grunnlag for: 1) Den/de dataansvarliges behandling av personopplysninger 2) Overføring av personopplysninger		N/A
7.4.a.2	Den dataansvarlige og databehandler har begge et selvstendig ansvar for at behandling av personopplysninger i skytjenester dokumenteres i den regionale protokollen over behandlingsaktiviteter (Medinsight).		N/A
7.4.a.3	Skyleverandør skal bidra med informasjon om hvordan de behandler personopplysninger på vegne av dataansvarlig, slik at dataansvarlig kan ivareta sin forpliktelse til å gi informasjon til de registrerte gjennom en personvernerklæring, som beskrevet i GDPR artikkel 13.		DSP-11 DSP-12 DSP-15

7.4.1 Innebygd personvern

Dataansvarlig skal stille krav til at databehandler etterlever krav til innebygd personvern og personvern som standardinnstilling

#	Hovedprinsipp	Business Driver	Kilde
7.4.1.a	Databehandler skal sørge for at løsningen ivaretar innebygd personvern (Privacy by design).	BD1 BD4	RSS GDPR art. 25 Normen kapittel 4.3
#	**Delprinsipp**		**CAIQ Control ID**
7.4.1.a.1	Innebygd personvern og personvern som standardinnstilling skal ivaretas i designprosessen av en applikasjon. Innebygd personvern er nærmere beskrevet på sidene til Datatilsynet.		DSP-08

Ved behandling av personopplysninger kan det utløses krav om gjennomføring av personvernkonsekvensvurdering (DPIA).

Nærmere informasjon om personvernkonsekvensvurdering finnes på siden Personvern i Sykehuspartner.

7.4.2 Personvernkonsekvensvurdering

#	Hovedprinsipp	Business Driver	Kilde
7.4.2.a	Det skal gjennomføres GDPR-beslutningslogg. Dersom nødvendig skal dataansvarlig gjennomføre personvernkonsekvensvurdering (DPIA)	BD1 BD4	RSS GDPR art. 35 ISMS

7.4.3 Behandlingens lokasjon

#	Hovedprinsipp	Business Driver	Kilde
7.4.3.a	Skyleverandør skal tydelig informere om, og skriftlig dokumentere, den geografiske lokasjonen (land) der behandling av personopplysninger skjer. Med behandling menes blant annet prosessering, lagrede data, fjernaksess, support/vedlikehold, sletting og data i transport.	BD1 BD4	RSS GDPR art. 27
#	Hovedprinsipp	Business Driver	Kilde
7.4.3.b	Databehandling skal kun foregå dersom man kan oppnå tilstrekkelig personvern.	BD1 BD4	RSS

#	Delprinsipp	CAIQ Control ID
7.4.3.b.1	Behandling i tredjeland kan skje dersom helseforetakene og Sykehuspartner har godkjent behandlingen og overføringen er basert på et gyldig overføringsgrunnlag. Dette gjelder også i de tilfeller underleverandør har eierskap i tredjeland. Dette kan blant annet være ett av vilkårene nedenfor: • Behandlingen av personopplysninger skjer i en stat som Europakommisjonen har funnet til å ha tilstrekkelig vernenivå, se EU's Adequacy decisions. • Behandlingen skjer av et selskap som har tatt EUs standardpersonvernbestemmelser (Standard Contractual Clauses) inn i sin avtale med dataansvarlig. SCC alene er ikke nødvendigvis tilstrekkelig, og ytterligere tiltak må vurderes. • Behandlingen skjer på bakgrunn av Binding Corporate Rules (BCR) hvor selskapet er etablert i EU/EØS og innenfor sitt konglomerat overfører personopplysninger ut av EU/EØS. BCR må være godkjent av kompetent tilsynsmyndighet.	N/A
7.4.3.b.2	Det må vurderes om behandlingen av personopplysninger i tredjeland ivaretar et tilsvarende beskyttelsesnivå for personopplysningene som innenfor EU/EØS, jf. EDPBs retningslinjer. Dette gjøres ved å bruke SPHFs veileder for overføringer til tredjeland.	GRC-01 GRC-02
7.4.3.b.3	Dersom leverandør overfører personopplysninger til ikke godkjente tredjeland, skal leverandøren oppgi hvilket overføringsgrunnlag som benyttes for overføringen.	
7.4.3.b.4	Behandling av informasjon i stater der etterretningsrisikoen vurderes som høy bør unngås (se NO-41 Liste over høyrisikoland)	N/A

7.4.4 Segmentering av data

Skyleverandøren skal ha tekniske mekanismer som sikrer tilfredsstillende skille mellom data fra ulike dataansvarlige i skyleverandørens tekniske infrastruktur. De tekniske mekanismene skal være dokumentert. Feil på teknisk oppsett eller andre brudd på personopplysningssikkerheten som berører én av skyleverandørens kunder, for eksempel feil tilgangsstyring, skal ikke kunne ha negative konsekvenser for leverandørens øvrige kunder.

#	Hovedprinsipp	Business Driver	Kilde
7.4.4.a	Skyleverandøren skal sikre at personopplysninger fra ulike dataansvarlige skilles på en tilfredsstillende måte, enten fysisk eller logisk.	BD1 BD4	RSS
#	Delprinsipp		CAIQ Control ID
7.4.4.a.1	Skyleverandørens tekniske mekanismer for segmentering av data skal være skriftlig dokumentert og tilgjengelig for SPHF.		IVS-06

7.5 Revisjon

For å vise etterlevelse eller påpeke mangler mot gitte krav relatert til informasjonssikkerhet og personvern i forskrift, standarder, policyer eller rutiner skal det gjennomføres revisjoner av skyleverandøren og tilbudte tjenester.

De fleste skyleverandører utsteder tredjepartsattestasjoner der uavhengige tredjeparter utfører regelmessig revisjon av deres leverte tjenester. Så lenge en skyleverandør har en slik tredjepartsattestasjon, som dekker levert tjeneste, bør SPHF søke å få tilgang til denne. En slik rapport starter som oftest med en selvdeklarering fra leverandøren etterfulgt av at revisor tester utførelsen av kontroller på leverandørens tjeneste.

#	Hovedprinsipp	Business Driver	Kilde
7.5.a	Det skal gjennomføres revisjon av leverandører og tjenestene de leverer til HF i regionen	BD1, BD4, BD7	RSS Normen kapittel 5.4.6
#	Delprinsipp		CAIQ Control ID
7.5.a.1	Revisjon av skytjenesten skal gjennomføres jevnlig som en del av øvrige aktiviteter innen sikkerhetsrevisjon i SPHF.		A&A-01.2
7.5.a.2	Revisjonsmetode skal være kontraktsfestet og det kan velges en eller flere av følgende metoder: - Leverandøren selvdeklarerer (internrevisjon) - Uavhengig tredjepart reviderer (attestasjon) - Kunden får adgang til å gjennomføre revisjon på egenhånd SPHF bør i de fleste tilfeller søke å få en attestasjon fra en uavhengig tredjepart for levert tjeneste.		A&A-05.1 STA- 09.1

7.5.a.3	Skyleverandør skal ha dokumentert hvordan de sikrer kontinuerlig etterlevelse av relevante krav og regelverk. Dette skal kunne leveres til SPHF på forespørsel.	A&A-04.1

7.6 Dataklassifisering

#	Hovedprinsipp	Business Driver	Kilde
7.6.a	Dataansvarlig skal klassifisere data i henhold til gjeldende modell for informasjonsklassifisering hentet fra Ledelsessystem for Informasjonssikkerhet. Data skal sikres i henhold til gitt klassifisering.	BD1, BD4	RSS
#	Delprinsipp		CAIQ Control ID
7.6.a.1	For tjenester med høy og svært høy verdi bør følgende sikkerhetsmekanismer vurderes: - CASB (reversed proxy) - DLP - DMZ - Mikrosegmentering - Kryptering		UEM-10.1 UEM-11.1 CEK-03

7.7 Tilgangsstyring (IAM)

Tilgangsstyring til skytjenester skal etableres i henhold til målarkitektur for Identity and Access Management (IAM). Tilgang til skytjenester skal bare gis til brukere med tjenstlig behov.

Sykehuspartner HF er utøvende ansvarlig for identitetsforvaltning i Helse Sør-Øst og PAGAID er autorativ kilde for unike identifikatorer for ansatte i Helse Sør-Øst.

7.7.1 Autorisering og autentisering

#	Hovedprinsipp	Business Driver	Kilde
7.7.1.a	Tilgang til skytjenester skal gis basert på SPHFs identiteter og autentiseres via SPHFs regionale autentiseringstjeneste.	BD1, BD2, BD3, BD4	RSS ISMS Normen kapittel 5.2
#	Delprinsipp		CAIQ Control ID
7.7.1.a.1	Skytjenesten skal være identitetsføderert slik at autentisering skjer via SPHFs regionale autentiseringstjeneste.		N/A
7.7.1.a.2	Hvis skytjenesten har funksjonalitet for å invitere inn identiteter fra andre virksomheter (utenfor HSØ), så må den eksterne virksomheten autentisere sine identiteter ved identitetsføderering. Det skal ikke opprettes lokale brukerdatabaser. Eksempelvis Dersom det opprettes et samarbeid med en annen helseregion (Helse Vest) om deling av informasjon som ligger i en løsning SPHF har anskaffet så skal da den andre regionenes identiteter identitetsfødereres inn. For å få til dette samarbeidet om data så må det opprettes avtaleverk for å regulere hvem som skal ha tilgang og hvilke under hvilke forutsettinger.		N/A
7.7.1.a.3	Autorisering av brukere skal vedlikeholdes i SPHF autoriseringstjeneste i henhold til IAM Målarkitektur, og synkroniseres til skyen kontinuerlig.		N/A
7.7.1.a.4	Skytjenester skal minimum benytte autentiseringsnivå betydelig (Regional autentiseringspolicy for Helse Sør-Øst (sykehuspartner.no)		N/A

7.7.2 Separation of duties

#	Hovedprinsipp	Business Driver	Kilde
7.7.2.a	Brukere av tjenesten skal aldri ha flere rettigheter enn de har tjenstlig behov for. Tydelig adskilte roller må ivaretas i tjenesten.	BD4, BD7	RSS
#	Delprinsipp		CAIQ Control ID
7.7.2.a.1	Tilganger for Helse Sør-Øst-brukere skal begrenses for å forhindre uautorisert tilgang til systemer eller data.		IAM-05.1

7.7.3 Administrative/privilegerte tilganger

Skyleverandør kan benytte egne privilegerte tilganger for å vedlikeholde egen plattform uten at det påvirker kundens data. Dersom skyleverandør har behov for tilgang til kundens data, må kunden godkjenne tilgangen.

#	Hovedprinsipp	Business Driver	Kilde
7.7.3.a	Leverandørens bruk av administrative- og privilegerte tilganger i HSØ-skyinfrastruktur/-tjenester skal praktiseres etter prinsippet om «least privilege».	BD1, BD4, BD7	RSS
#	Delprinsipp		CAIQ Control ID
7.7.3.a.1	Leverandørs bruk av administrative- eller privilegerte tilganger skal spores og logges.		LOG-02.1
7.7.3.a.2	Leverandørens administrative tilganger i skytjenesten skal i størst mulig grad begrenses og tilgangen til kundens data skal være godkjent av kunden. Just-in-Time-Access skal benyttes om mulig.		IAM-10.1 IAM-10.2
7.7.3.a.3	Skyleverandøren kan vedlikeholde plattformen uten godkjenning av kunden, så lenge det ikke påvirker kundens data.		IAM-11.1
#	Hovedprinsipp	Business Driver	Kilde
7.7.3.b	Ansatte i HSØ som skal ha privilegerte tilganger til en skytjeneste skal kun gis tilganger via HSØ sin etablerte driftsløsning for privilegerte tilganger (PAM), eller tilsvarende funksjonalitet hvor SPHF har kontroll og utsteder rettigheter og tilganger.	BD1, BD4, BD7	RSS
#	Delprinsipp		CAIQ Control ID
7.7.3.b.1	Tjenstlig behov for privilegerte tilganger til skytjenester skal dokumenteres for den enkelte tjeneste.		IAM-05.1
7.7.3.b.2	Administrative- eller privilegerte tilganger i en skytjeneste skal håndteres tilsvarende som om tjenesten var etablert on-premise.		N/A

7.7.4 Kontroll av tilganger

#	Hovedprinsipp	Business Driver	Kilde
7.7.4.a	Det skal gjøres jevnlig kontroll av tilganger i skytjenesten.	BD1, BD4	RSS

7.8 Fysisk sikkerhet/adgangskontroll

Det er skyleverandør som er utøvende ansvarlig for fysisk sikkerhet til sine anlegg, mens det respektive helseforetak selv er endelig ansvarlig for sin informasjon, uavhengig av hvor den er lagret. SPHF må derfor, på vegne av foretakene i regionen, be leverandør fremskaffe nødvendig dokumentasjon på at tiltak knyttet til fysisk sikring er i henhold til gjeldende lovverk, nasjonale føringer og gjeldende anbefalinger.

#	Hovedprinsipp	Business Driver	Kilde
7.8.a	Skyleverandør skal dokumentere at fysisk sikring av lokaler og utstyr.	BD12	RSS Normen kapittel 5.3 og 5.7.5
#	**Delprinsipp**		**CAIQ Control ID**
7.8.a.1	Skyleverandør skal dokumentere at fysisk sikring, inkludert perimetersikring og adgangskontroll, er i henhold til etablerte anerkjente standarder eller rammeverk som omtaler sikring av datasenter (f.eks. ISO TS 22237, ISO27001, CSA Star certification, PCI DSS mv.)		DCS-07.1 DCS-07.2
7.8.a.2	Skyleverandør skal dokumentere at det foreligger godkjente, oppdaterte og utprøvde (testede) beredskapsplaner, kontinuitetsplaner og kriseplaner som ivaretar fysiske forhold. Se kapittel 7.13 Business Continuity, tilgjengelighet og oppetid i dette dokumentet for ytterligere prinsipper knyttet til dette.		DCS-12 DCS-15 BCR-03 BCR-04 BCR-06 BCR-09 BCR-10

7.9 Monitorering, logging og deteksjon

Sykehuspartner HF og SPHF CERT har en sentral rolle for å ivareta operative sikkerhetsfunksjoner i Helse Sør-Øst.

Det vil være nødvendig å tilpasse og videreutvikle SPHFs evne til å drive tilstrekkelig monitorering, logging og deteksjon i forbindelse med skytjenester.

#	Hovedprinsipp	Business Driver	Kilde
7.9.a	Monitorering, logging og deteksjonsaktivitet skal integreres i SPHFs eksisterende regime. Tjenesteleverandør skal tilrettelegge for hensiktsmessig avlevering eller tilgang til funksjoner som gjør det mulig å ha sporbarhet og uavviselighet til handlinger utført i tjenesten.	BD1 BD3 BD4 BD10	RSS
#	Delprinsipp		CAIQ Control ID
7.9.a.1	Loggmateriale fra skytjenesten skal være strukturert slik at det tydelig fremkommer hvilken aktivitet som er utført. Loggene skal være i RFC 5424-format.		LOG-03 LOG-08
7.9.a.2	Som minstekrav skal tilgangsstyringslogger, transaksjonslogger og aktivitetslogger være tilgjengelig for å sikre sporbarhet og uavviselighet.		LOG-01.1 LOG-05.1
7.9.a.3	Sikkerhetskapabiliteter mht. monitorering, logging og deteksjon skal være etablert i skytjenesten. eksempelvis brannmur, Intrusion Detection System (IDS), Intrution Prevention System (IPS), Extended Detection and Response (XDR).		TVM-01.1

7.10 Hendelseshåndtering og etterforskning

#	Hovedprinsipp	Business Driver	Kilde
7.10.a	Hendelseshåndtering og –etterforskning knyttet til skytjenester forutsetter at SPHF CERT har anledning til å benytte sine verktøy og metoder ved hendelser som kan påvirke konfidensialitet, integritet eller tilgjengelighet i tjenesten.	BD4 BD7 BD8 BD12	RSS
#	Delprinsipp		CAIQ Control ID
7.10.a.1	Hendelseshåndtering knyttet til den respektive skytjeneste må tilrettelegge for instrumentert styring fra operative sikkerhetsressurser. Avtaler, rutiner og prosedyrer skal være etablert.		SEF-03.1
7.10.a.2	Det skal fremgå i avtaletekst for skytjenesten at skyleverandør skal gjøre nødvendige logger umiddelbart tilgjengelig for SPHF CERT hvor dette er nødvendig for hendelseshåndtering og –etterforskning.		SEF-02.1
7.10.a.3	Skytjenestens Disaster Recovery Plan skal omfatte hendelseshåndtering og –etterforskning.		BCR-01
#	Hovedprinsipp	Business Driver	Kilde
7.10.b	Dokumentasjon tilhørende skytjenesten skal inneholde en beskrivelse av leverandørens kommunikasjonskanal til SPHF CERT.	BD4 BD7 BD8 BD12	RSS
#	Delprinsipp		CAIQ Control ID
7.10.b.1	Hendelser som påvirker skytjenestens ivaretagelse av konfidensialitet, integritet eller tilgjengelighet skal meldes gjennom konkret avtalt grensesnitt, uten ugrunnet opphold, til SPHF CERT.		BCR-07.1 SEF-07.1

7.11 Trussel- og sårbarhetshåndtering

#	Hovedprinsipp	Business Driver	Kilde
7.11.a	Ansvarsmatrisen i kapittel 7.1.1 er grunnleggende for å definere hvem som skal ivareta trussel- og sårbarhetshåndtering i alle typer tjeneste- og leveransemodeller.	BD1, BD4, BD5, BD7, BD8, BD10, BD12	RSS
#	Delprinsipp		CAIQ Control ID
7.11.a.1	Håndtering av sårbarheter og trusler skal følge ansvarsmatrisen.		N/A

7.11.a.2	Sikkerhetstesting skal inkluderes i tjenesteleveransen, og det skal være etablerte prosesser for å:
	- Identifisere sårbarheter (ikke begrenset til):
	  ○ Sårbarhetsscanning
	  ○ Penetrasjonstester
	- Vurdere sårbarheter
	- Håndtere sårbarheter
			TVM-01.1

7.12 Endringshåndtering

#	Hovedprinsipp	Business Driver	Kilde
7.12.a	Alle tjenester som tas i bruk i skyen må følge gjeldende prosess for endringshåndtering.	BD1, BD5	RSS Normen kap.5.4.2
#	Delprinsipp		CAIQ Control ID
7.12.a.1	Endringer i skytjenester dokumenteres og håndteres i en risikobasert tilnærming.		CCC-03.1
7.12.a.2	Avtalen med skyleverandør må beskrive prosess og kommunikasjonskanal mellom Sykehuspartner HF og skyleverandør, slik at endringshåndtering blir ivaretatt.		CCC-05.1

7.13 Business Continuity, tilgjengelighet og oppetid

Dette kapittelet handler primært om planverk knyttet til beredskap, kontinuitet og kriser. Kapittelet må sees i sammenheng med kapitlene 7.6 Dataklassifisering og 7.9 Monitorering, logging og deteksjon, som omtaler mer operasjonelle sider knyttet til klassifisering og overvåking. Videre er det særlig viktig å se det i sammenheng med «Ansvarsmatrise Sikkerhetstiltak Skytjenester» som beskrevet i kapittel 7.1.1 Ansvarsfordeling for sikkerhetstiltak og valgt tjenestemodell.

#	Hovedprinsipp	Business Driver	Kilde
7.13.a	Skytjenester skal beskyttes mot bortfall og uønsket nedetid ved hjelp av egnede beredskapsplaner. Det skal foreligge beredskapsplaner for skytjenester.	BD1 BD2 BD3 BD5	RSS Normen kapittel 5.9
#	Delprinsipp		CAIQ Control ID
7.13.a.1	Gjenoppretningsplan ved kriser (DRP) skal etableres per tjeneste og dokumenteres i HelseCIM. Innholdet i DRP skal være i henhold til verdien til tjenesten. Varslingsrutiner for hendelser skal også fremkomme i planverket. DRP skal være oppdatert og testes i planlagte intervaller.		BCR-01.1 BCR-01.2 BCR-04.1
7.13.a.2	Ansvarsfordeling for gjenoppretning ved kriser skal være basert på tjenestemodell, og det skal i DRP tydelig fremkomme ansvarsområdene og -fordelingen mellom skyleverandør og kunden.		N/A
7.13.a.3	På bakgrunn av skytjenestens klassifisering må hensiktsmessige tiltak for å forhindre tap av data implementeres. Recovery point objective (RPO) og recovery time objective (RTO) fastsettes basert på tjenestens kritikalitet.		BCR-08.1 BCR-08.2

7.14 Livssyklushåndtering

#	Hovedprinsipp	Business Driver	Kilde
7.14.a	Tjenesteutsetting krever at dataansvarlig og databehandler har kontroll over livssyklusen til data.	BD1, BD4, BD6	RSS
#	Delprinsipp		CAIQ Control ID
7.14.a.1	Tjenesteansvarlig vil være forvalter av livssyklushåndtering for tjenesten.		N/A
7.14.a.2	Alle tjenester skal ha en definert livssyklus dokumentasjon.		DCS-01.1
7.14.a.3	Skyleverandør skal dokumentere at de har policyer og prosedyrer for sikker avhending eller gjenbruk av ressurser, herunder utstyr, lagring, filer og minne mv.		DCS-01.1
7.14.a.4	Det skal dokumenteres hvilke data som behandles i tjenesten og definert levetid på data.		N/A

7.15 Kryptering og nøkkelhåndtering

#	Hovedprinsipp	Business Driver	Kilde
7.15.a	Kryptering kan i enkelte tilfeller være et godt tiltak for å ivareta konfidensialiteten til data. Det skal benyttes anbefalte kryptografiske standarder. Kilder for egnet kryptografisk beskyttelse kan være Nasjonal Sikkerhetsmyndighets Cryptographic Recommendations eller NIST sin krypteringsstandard.	BD1, BD3	EDPB[1] RSS Normen kapittel 5.3.5
#	Delprinsipp		CAIQ Control ID
7.15.a.1	Behov for kryptering og eierskap av nøklene skal fremkomme av informasjonsklassifiseringen og EU/tredjeland bestemmelser. For tredjeland bør BYOK sterkt vurderes for å redusere konsekvensen ved innsynsbegjæring eller annen sekundær bruk av data. En skal ta stilling til: - Behov for å ivareta informasjonens konfidensialitet og integritet Identifiserte risikodrivende faktorer som for eksempel overføring av informasjon til tredjeland - Behov for kryptering under transport, lagring og prosessering. - Krypteringsstandard - Nøkkelstyrke - Bring-your-own-Key (BYOK), Bring-your-own-Encryption (BYOE)		CEK-03.1 CEK-04.1

7.16 Human Resource-sikkerhet

#	Hovedprinsipp	Business Driver	Kilde
7.16.a	Leverandør skal påse at sine ansatte har riktig kompetanse til å utføre sine arbeidsoppgaver og at de er sikkerhetsmessig skikket. Videre skal leverandør videreføre dette kravet til sine underleverandører.	BD1 BD4 BD8 BD12	RSS Normen kapittel 5.1 eIDAS-forordningen
#	Delprinsipp		CAIQ Control ID
7.16.a.1	Alle ansatte, som skal jobbe med tjenesten, skal ha signert taushetserklæring. Det er preferert å bruke SPHFs regionale sikkerhetsinstruks.		HRS-07.1

7.17 Infrastruktur og virtualisering

7.17.1 Infrastruktur

#	Hovedprinsipp	Business Driver	Kilde
7.17.1.a	SPHF skal utnytte skyens kapabiliteter for å sikre robusthet i tjenesten.	BD1, BD4, BD9, BD11	RSS ISMS Normen kap. 5.4
#	Delprinsipp		CAIQ Control ID
7.17.1.a.1	Skytjenesten skal hvor det er mulig etterstrebe zero trust.		N/A
7.17.1.a.2	Skytjenester som er tilgjengelige fra internett skal benytte DMZ og etterstrebe tre-lags arkitektur.		N/A
7.17.1.a.3	Produksjonsmiljøer og ikke-produksjonsmiljøer skal skilles fysisk og/eller logisk.		IVS-05.1
#	Hovedprinsipp	Business Driver	Kilde
7.17.1.b	Miljøer skal, så langt det er mulig, benytte standardiserte oppsett og konfigurasjon basert på Helse Sør-Øst sine krav, eventuelle nasjonale krav og beste praksis i markedet for øvrig.	BD1, BD4, BD11	RSS ISMS Normen kap. 5.4
#	Delprinsipp		CAIQ Control ID
7.17.1.b.1	Skytjenesten skal være herdet, uavhengig av tjeneste- eller leveransemodell. Der det er mulig skal Center for Internet Security sine herdede og pre-konfigurerte oppsett benyttes for skytjenester (CIS Hardened Images).		IVS-04.1
7.17.1.b.2	Alle miljøer skal ha sikring som er dimensjonert for informasjonen som forvaltes i dem og kritikaliteten til løsningene som kjører i dem. Dette gjelder også test- og utviklingsmiljøer.		N/A

7.18 Applikasjonssikkerhet

IaaS- og PaaS-tjenester hvor det skal utvikles en applikasjon, må etterleve sikkerhetskrav i henhold til applikasjonsutvikling.

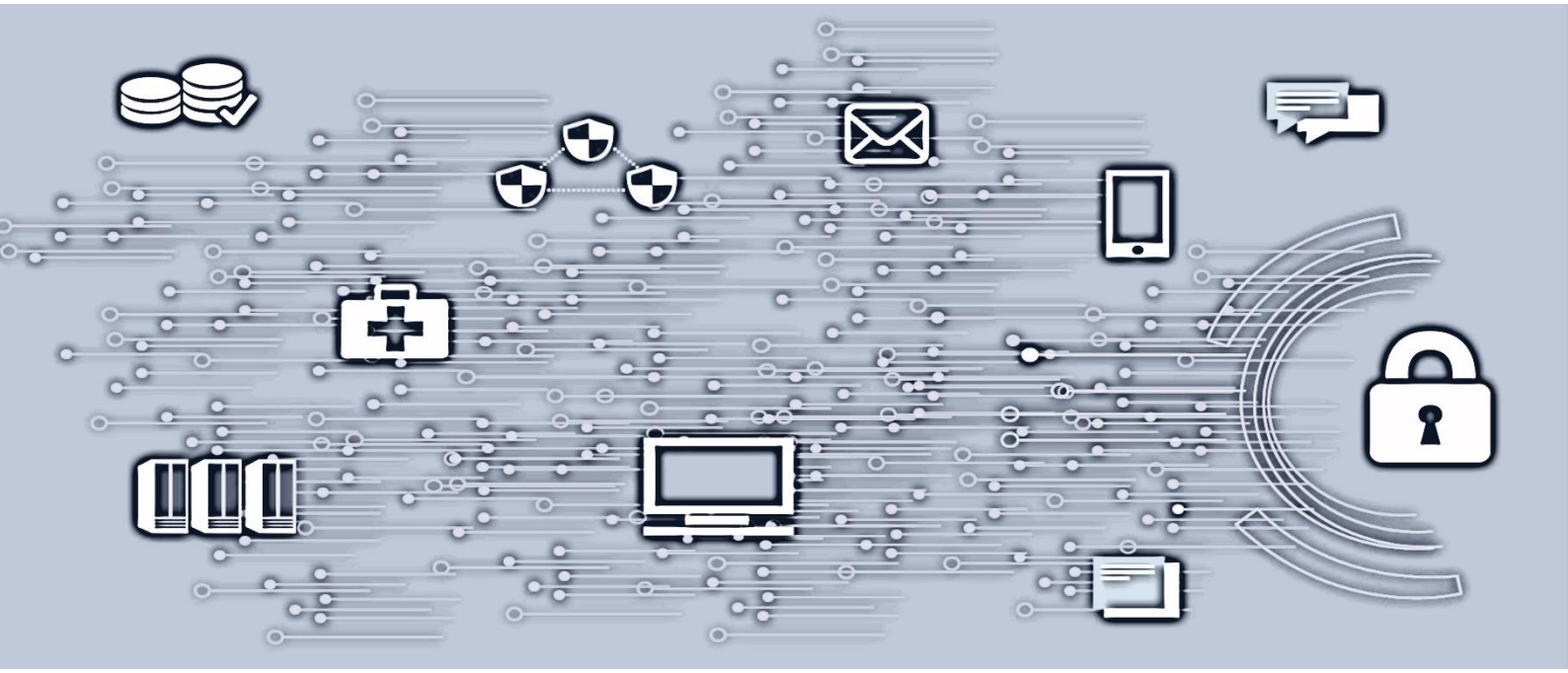
#	Hovedprinsipp	Business Driver	Kilde
7.18.a	Tjenesten med tilhørende applikasjoner og API-er skal designes, utvikles og testes, og være gjenstand for kontinuerlig forbedring.	BD4 BD9 BD11	RSS ISMS
#	Delprinsipp		CAIQ Control ID
7.18.a.1	Sikkerhet skal inkluderes i designprosessen av en applikasjon basert på industristandarder (tilsvarende OWASP, ISO 27034, SAFECODE).		AIS-04.1
7.18.a.2	Sikkerhetstesting (eksempelvis SAST og DAST) skal inkluderes i applikasjonsutviklingsprosessen.		AIS-07.1
7.18.a.3	Dataintegritet skal være ivaretatt gjennom livssyklusen av applikasjonen.		N/A
#	Hovedprinsipp	Business Driver	Kilde
7.18.b	Applikasjoner skal forvaltes i tråd med valgt tjenestemodell.	BD4 BD9 BD11	RSS ISMS Normen kapittel 5.3.5
#	Delprinsipp		CAIQ Control ID
7.18.b.1	Roller og ansvar knyttet til applikasjonsforvaltning hos SPHF skal baseres på valgt tjenestemodell og være tydelig definert.		STA-01.1
7.18.b.2	Applikasjoner skal modelleres inn i uCMDB i henhold til gjeldende tjenesteinformasjonsmodell (TIM-modell).		N/A
7.18.b.3	Basert på applikasjonens kritikalitet og klassifisering av informasjon som behandles, skal overvåking og deteksjon av applikasjonen vurderes.		N/A

7.19 Interoperabilitet og portabilitet

#	Hovedprinsipp	Business Driver	Kilde
7.19.a	Data i skytjenester skal i størst mulig grad basere seg på standardiserte- og maskinlesbare format for å understøtte forretningsbehovene.	BD4 BD5 BD6 BD8 BD9 BD10	RSS

SYKEHUSPARTNER

Regional sikkerhetspolicy for skytjenester



Innhold

Versjon	Dato	Godkjent av
1.0	02.10.2020	Christian Jacobsen
1.01	08.04.2021	Christian Jacobsen
1.02	21.05.2021	Christian Jacobsen
1.1	14.02.2022	Christian Jacobsen

1 Introduksjon

Bruk av skytjenester skal kunne gi tilstrekkelig tilgjengelighet, god kvalitet og sikkerhet i driftstjenester samtidig som det effektivt understøtter helseforetakenes behov. En sikkerhetsarkitektur for skytjenester er en forutsetning for at dette skal kunne oppfylles.

Denne sikkerhetsarkitekturen har vi valgt å kalle «Grunnmur for skytjenester». Dokumentene som utgjør «Grunnmur for skytjenester» ligger i det regionale ISMS. Det er et sett med basiskapabiliteter som beskriver informasjonssikkerhet og personvernstiltak for hvordan skytjenester tas i bruk, inkludert bla. tilgangsstyring, risikostyring, leverandørhåndtering, sikkerhetskrav, personvern og endring- og hendelseshåndtering.

Grunnmur for skytjenester skal understøtte tjenester som etableres i skyen uansett tjeneste- og leveransemodell.

2 Formål og scope

Formålet med regional sikkerhetspolicy for skytjenester er å sammenfatte og befeste de styrende forhold som gjør seg gjeldende for Helse Sør-Øst sin bruk av skytjenester. Hensikten er å ivareta informasjonssikkerhets- og personvernmessige forhold ved bruk av skytjenester uavhengig av hvilken type data som behandles.

Dokumentet beskriver krav til fellestjenester i skyen i tillegg til et sett med basistjenester.

2.1 Målgruppe

Regional sikkerhetspolicy for skytjenester skal vise «de store linjene» – altså en oversiktlig fremstilling av hvilke områder som skal hensyntas når et program, prosjekt eller foretak ønsker å ta i bruk skytjenester.

Dokumentet er hovedsakelig ment å treffe ledere og prosjektledere som oftest sitter med beslutningsmyndighet og må forholde seg til prinsipielle eller strategiske valg i sitt virke.

Dokumentet må likevel leses i sammenheng med NO-30 Regionale sikkerhetsprinsipper og –krav for skytjenester (RSPS), som detaljerer og tydeliggjør krav som utledes fra dette dokumentet.

2.2 Virkeområde

Dokumentet gjelder for de leveranser eller tjenester som på en eller annen måte omfatter bruk av skytjenester i Helse Sør-Øst.

2.3 Avhengigheter og forutsetninger

I de tilfeller dette dokumentet påpeker manglende styrende dokumentasjon i regionen, må dette utarbeides for å dekke de mangler som fremkommer.

3 Kilder

3.1 Lovverk og styrende dokumentasjon

Hovedkildene til krav for informasjonssikkerhet i skytjenester hentes fra (ikke uttømmende):

- Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren v.6
- NSM – Grunnprinsipper for IKT sikkerhet v.2

- Arkivlova[1]
- Bokføringsloven
- Personopplysningsloven og personvernforordningen (GDPR)
- Pasientjournalloven, Helseregisterloven og Helsepersonelloven

3.2 Rammeverk og standarder

Hovedkilde til rammeverk som benyttes for HSØ hentes fra:

- SABSA – Sikkerhetsarkitektur rammeverk
- Cloud Security Alliance – kontrollrammeverk for skytjenester
- Security Guidance for Critical Areas of Focus in Cloud Computing v4.0
- CSA – Cloud Control Matrix (ivaretar delvis ISO27001/ISO27018)

3.3 Interne og eksterne strategier

Kilder til forretningsbehov:

- Nasjonal strategi for bruk av skytjenester
- Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten
- Veileder i bruk av skytjenester til behandling av helse- og personopplysninger
- Målarkitektur for IAM (internt dokument)
- Tilnærming for bruk av skytjenester (internt dokument)

4 Forkortelser og begreper

Forkortelse/ begrep	Fullt navn/forklaring
ASR	Arkitektur i program og prosjekter
AWS	Amazon Web Services
CAIQ	Consensus Assessment Initiative Questionaire
CASB	Cloud Access Security Broker
CCM	Cloud Control Matrix
Community cloud	Skytjenester for fellesskap av virksomheter
CSA	Cloud Security Alliance
DBA	Databehandleravtale
DevOps	Software Development and Information Technology Operations
DLP	Data Loss Prevention
eIDAS	Electronic Identification, Authentication and Trust Services. EU regulativ om elektronisk ID.
EMM	Enterprise Mobility Management
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation (personvernforordningen)
HF	Helseforetakene under Helse Sør-Øst inkludert Sykehuspartner

[1] NOU 2019:9 legger grunnlag for ny arkivlov. Dette skal tas hensyn til i dette dokumentet når ny arkivlov foreligger.

Helseforetakene i regionen	Her menes alle HF, inkludert Sykehuspartner HF og Helse Sør-Øst RHF.
HSØ	Helse Sør-Øst RHF
Hybrid cloud	Kombinasjon av private og public cloud. Både eksklusive og delte skytjenester
IaaS	Infrastructure-as-a-Service
IAM	Identity and Access Management
ISMS	Information Security Management System
Leveransemodell sky	Typen leveranse av sky: private/public/hybrid/community cloud
LG1	Ledermøtet SPHF
MA	Microsoft Azure
MAM	Mobile Application Management
MDM	Mobile Device Management
MFA	Multi Factor Authentication
NDA	Non-Disclosure Agreement
NKOM	Nasjonal kommunikasjonsmyndighet
NSM	Nasjonal Sikkerhetsmyndighet
PaaS	Platform-as-a-Service
PKV	Personvernkonsekvensvurdering (DPIA)
Private cloud	Skytjenester tilbudt eksklusivt for en (isolert) virksomhet
Public cloud	Skytjenester som deles mellom flere virksomheter
RPO	Recovery Point Objective – Største akseptable datatap målt i tid, gir rammer for hvor ofte back-up skal tas.
RTO	Recovery Time Objective – Lengste akseptable nedetid i strekk, setter ambisjonsnivå for hvor fort tjenesten skal kunne gjenopprettes ved en feilsituasjon eller hendelse.
RSR	Regionalt Sikkerhetsfaglig Råd
RSS	Regional Sikkerhetspolicy for Skytjenester
RSPS	Regionale Sikkerhetsprinsipper for Skytjenester
RSV	Regionalt Sikkerhetsvurderings team
SaaS	Software-as-a-Service
SABSA	Sherwood Applied Business Security Architecture
SECaaS	Security-as-a-Service
SLA	Service Level Agreement
Skyleverandør	En skyleverandør tilbyr skybasert plattform, infrastruktur, program eller lagringstjenester
Skytjenste	Skytjenester er en samlebetegnelse for leveransemodeller som muliggjør tilgjengelige, tilpassede, «on-demand», tilgang til en pool med delte ressurser som kan skaleres opp eller ned (både for kunde og leverandør). Infrastrukturen som leverer skytjenesten kan være tilgjengelig både i egen infrastruktur, og via eksterne nettverk (utenfor virksomhetens infrastruktur).
SPARK	Sykehuspartner Arkitekturråd
SPHF	Sykehuspartner HF
TCO	Total Cost of Ownership

Tjenestemodell sky	Typen skytjeneste: IaaS, PaaS, SaaS
TOGAF	Arkitektur-rammeverk

5 SABSA rammeverk for sikkerhetsarkitektur

HSØ benytter TOGAF som rammeverk for arkitektur. I TOGAF håndteres sikkerhet og risiko gjennom krav til interessenter, og det kan derfor være nyttig med ytterligere detaljering og et eget rammeverk for sikkerhetsarkitektur. Beslutningen om å ta i bruk SABSA Sikkerhetsarkitektur som et tillegg til TOGAF ble tatt 14/11/2019 i LG1. Dokumentene som foreløpig utgjør en sikkerhetsarkitektur for skytjenester omtales som «Grunnmur for skytjenester» og oppbyggingen er basert på rammeverket SABSA.

SABSA supplerer med en forretnings- og risikobasert sikkerhetsarkitektur som en del av den overordnede virksomhetsarkitekturen. En SABSA-basert sikkerhetsarkitektur skal understøtte forretningen, noe som er i tråd med grunnprinsippene i TOGAF. SABSA kan dermed brukes som rammeverk for en sikkerhetsarkitektur uten at dette går på bekostning av en TOGAF-basert virksomhetsarkitektur.

SABSA rammeverket har en metode for å utvikle risikodrevne informasjonssikkerhets- og informasjonssikringsarkitekturer for virksomheter og for å levere løsninger som støtter viktige forretningsinitiativer. SABSA er gratis å bruke for alle, uten krav til lisensiering for sluttbrukerorganisasjoner. SABSA anvendes til å utvikle og implementere arkitekturer og løsninger.

SABSA-modellen består av seks lag som vist i tabellen nedenfor (Figur 1). Hvert lag representerer et perspektiv sett fra en aktør i prosessen med å spesifisere, designe, konstruere og bruke målarkitekturen.

Det er seks horisontale lag av abstraksjon i arkitekturmodellen (kontekstuell, konseptuell, logisk, fysisk, komponent og serviceadministrasjon). For hvert av de horisontale lagene svares det på spørsmålene hva, hvorfor, hvordan, hvem, hvor og når gjennom seks vertikale elementer. Dette gir en matrise på 6x6 som representerer hele modellen for sikkerhetsarkitektur (Figur 1). Det nederste laget, Service Management Architecture, må tolkes i detalj på alle de andre lagene. Dette laget får dermed også en tverrgående vertikal dimensjon.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Figur 1 SABSA Matrix

De øverste lagene i sikkerhetsarkitekturen Contextual, Conceptual og delvis Logical som ivaretar overordnede forretningsmål og beskriver drivere for sikkerhet finnes i Regional Sikkerhetspolicy for Skytjenester (RSS).

I Regionale sikkerhetsprinsipper og -krav for skytjenester (RSPS) fokuseres det på det logiske-, fysiske- og komponentlaget i Grunnmur for skytjenester. Dette inkluderer identifisering og spesifisering av logiske elementer og forholdet mellom dem, krav til fysiske elementer som støtter logiske elementer, og krav til spesifikke prosesser og verktøy.

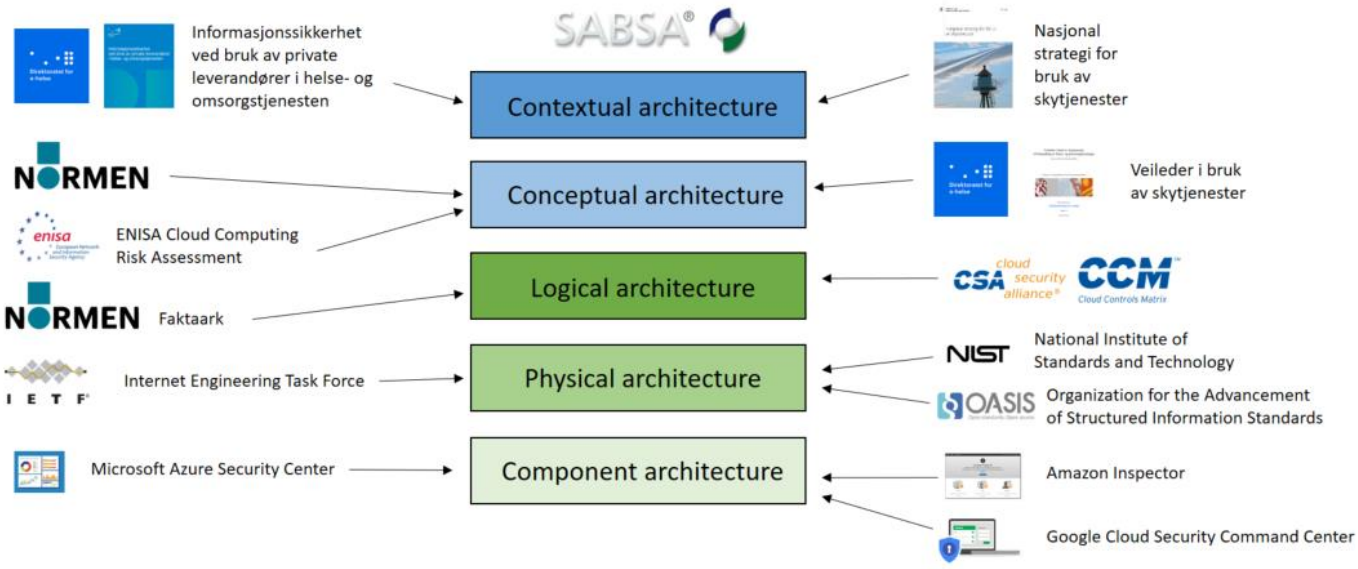
Ved å bruke SABSA får vi en toveis sporbarhet i Grunnmur for skytjenester. I policyen utledes forretningsbehovene ved bruk av skytjenester, som danner grunnlaget for drivere for sikkerhet. Deretter beskrives overordnede mål og behov for informasjonssikkerhet, verdier som må sikres og risikoer knyttet til drift og kjernevirksomhet. Slik kan vi sikre at forretningsbehov møtes ved å gå «nedover» i dokumentene gjennom krav og prinsipper helt til man har en konkret løsning på forretningsbehovene. På samme måte kan man starte med en konkret løsning og spore seg tilbake til krav, prinsipper og overordnede mål, og hva som var forretningsbehovet som drev dette i utgangspunktet.

5.1 SABSA for skytjenester

Som vist i Figur 2[2] er SABSA et rammeverk som kan binde sammen andre standarder og rammeverk på de ulike nivåene i arkitekturen. Nasjonale kilder til krav for skytjenester, kap. 3, kommer inn som

[2] Det vises i tegningen til NIST, OASIS, IETF. De har ikke vært brukt i dette dokumentet, men er med som eksempler.

en del av Contextual Architecture, mens internasjonale standarder gjerne benyttes som referanse for sikkerhetsmekanismer i Conceptual Architecture. Sikkerhetstiltak fra skyleverandørene er beskrevet i Component Architecture.



Figur 2 SABSA for skytjenester

6 Kontekstuell arkitektur

Dette kapittelet inneholder overordnede forretningsbehov og målsetninger relatert til bruk av skytjenester. De har som mål å knytte investeringen i sikkerhet og bruk av skytjenester både til eksterne retningslinjer for bruk av sky[3] og til SPHFs mål om sikre og stabile tjenester som kan standardiseres, moderniseres, digitaliseres og effektiviseres. De er hentet fra de autorative kildene nevnt i kapittel 3.

6.1 Forretningsbehov

Forretningsbehovene er formulert som funksjonelle krav. De er altså ikke absolutte krav, men overordnede målsetninger.

Drivere for sikkerhet, generelle prinsipper for- og tekniske krav til bruk av skytjenester skal kunne støtte opp under disse forretningsbehovene.

Krav #	Kravbeskrivelse	Kilde
R1	SPHF skal levere skytjenester som er kostnadseffektive å drifte i skyen.	Tilnærming for bruk av skytjenester
R2	Skytjenester skal gi Helse Sør-Øst ekstra kapasitet, fleksibilitet og robusthet	Tilnærming for bruk av skytjenester

[3] Nasjonal strategi for bruk av skytjenester

R3	SPHF skal vurdere å benytte tjenester som gir høyere kvalitet som skytjenester	Nasjonal strategi for bruk av skytjenester
R4	SPHF skal benytte tjenester i skyen som gir brukerne og foretakene i regionen økt sikkerhet	Nasjonal strategi for bruk av skytjenester
R5	SPHF må kunne tilby helseforetakene tjenester som kun er tilgjengelig i skyen (cloud native).	Normen
R6	Skytjenestene skal håndtere eksterne brukere på tilsvarende sikker måte slik tjenestene leveres i eget datasenter.	Normen
R7	Skytjenester skal legge til rette for samhandling. Dette gjelder bl.a. diskusjon, informasjonsdeling og videokonferanser.	Regional Sikkerhetspolicy for skytjenester
R8	Skytjenester skal legge til rette for virtuelle helsetjenester der kommunikasjon med pasient er sentralt.	Nasjonal strategi for bruk av skytjenester
R9	HSØ skal vurdere å benytte skytjenester som understøtter etablering av utviklingskapasitet i skyen basert på virtuelle maskiner eller kontainerteknologi.	Nasjonal strategi for bruk av skytjenester
R10	SPHF skal utvide testkapasitet ved å etablere testmiljøer i skytjenester.	Nasjonal strategi for bruk av skytjenester
R11	Skytjenester skal legge til rette for analyse og maskinlæring.	Nasjonal strategi for bruk av skytjenester
R12	Målarkitektur for IAM skal ivareta brukere uavhengig av lokasjon og på mobile klienter.	Målarkitektur for IAM
R13	Skytjenestene skal være fleksible og kunne utvides etter behov.	Veileder i bruk av skytjenester
R14	Styringssystemet skal kunne anvendes ved konsum av ulike tjenestemodeller i skyen, f.eks. Saas, Paas og IaaS.	Veileder i bruk av skytjenester
R15	Databehandleravtale med skyleverandør må tilfredsstille krav i personvernforordningen (GDPR).	Veileder i bruk av skytjenester
R16	Total Cost of Ownership (TCO), kost/nytte-vurdering, skal tas hensyn til når tjenester i skyen skal vurderes.	Nasjonal strategi for bruk av skytjenester
R17	SPHF skal ta i bruk skytjenester på en måte som gir nødvendig portabilitet og forutsigbare kostnader ved exit.	Nasjonal strategi for bruk av skytjenester
R18	Skytjenestene som konsumeres av SPHF skal leveres av leverandører som har relevante sertifiseringer eller kan dokumentere at de oppfyller standarder som er etablert for leveranser til HSØ.	Veileder i bruk av skytjenester
R19	Når SPHF etablerer skytjenester skal ansvar for utførelse av sikkerhetsoppgaver være avklart mellom SPHF, Helseforetak og Leverandør.	Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten
R20	Sikkerhet i skytjenester skal være i henhold til Normen, NSMs Grunnprinsipper for IKT sikkerhet og Regionens ledelsessystem for informasjonssikkerhet.	Veileder i bruk av skytjenester
R21	Skytjenester skal muliggjøre interoperabilitet og samarbeid, i et klinisk perspektiv, mellom foretakene i regionen for å understøtte prinsippet rundt «Èn pasient – èn journal».	Tilnærming til bruk av skytjenester

6.2 Drivere for sikkerhet

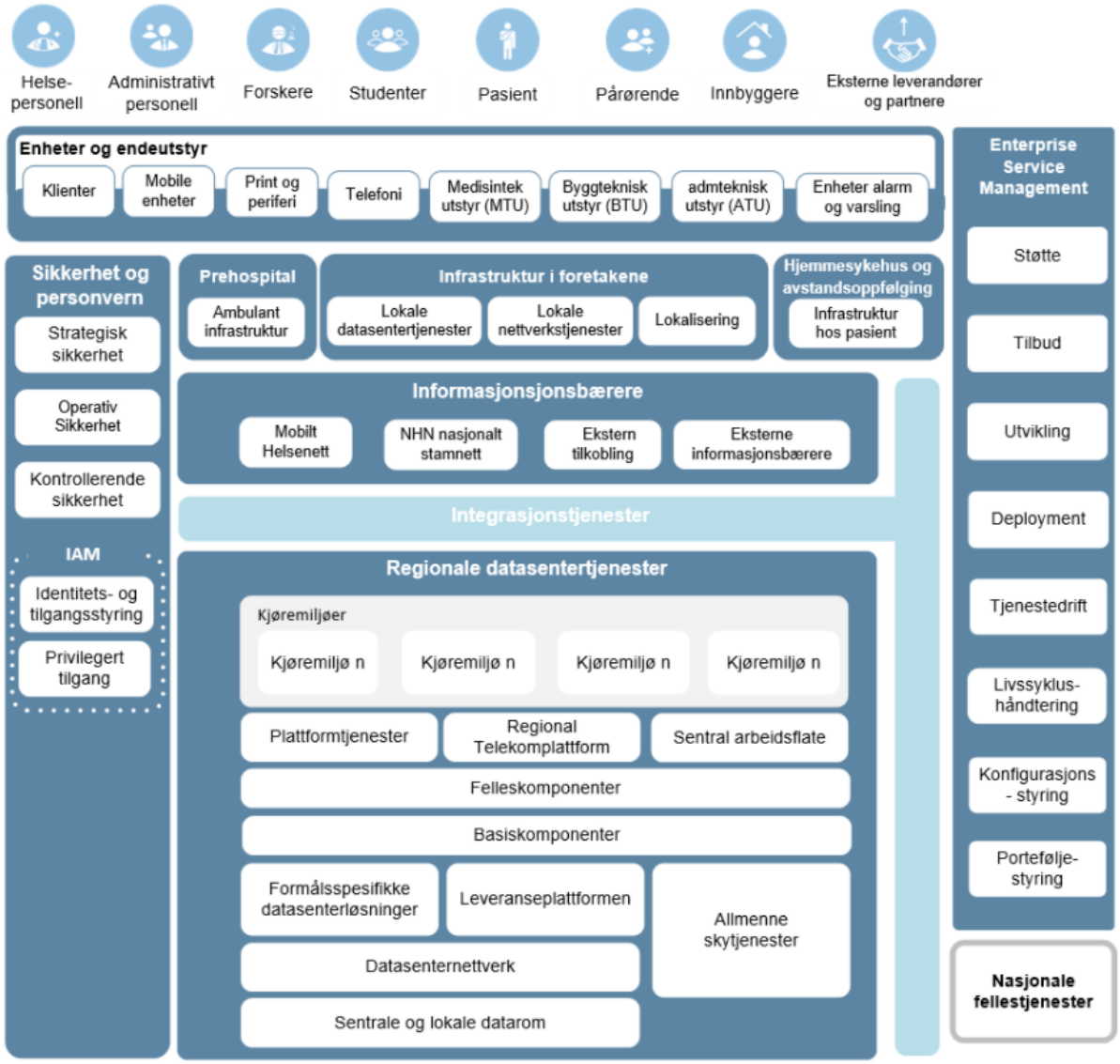
De funksjonelle kravene i kapittel 6.1 danner et grunnlag for drivere for sikkerhet. Driverne for sikkerhet er formulert som strategiske mål som implementeres for å støtte opp under spesifikke forretningsbehov og funksjonelle krav. Tabellen under lister opp driverne for sikkerhet og knytningen hver driver har til de funksjonelle kravene.

Driver#	Driver for sikkerhet - Beskrivelse	Knyttet til Krav#
BD1	Helseforetakene skal kunne ha tillit til at skytjenestene gir samme grad av konfidensialitet, integritet og tilgjengelighet som interne tjenester.	R4, R6, R15, R18, R20
BD2	Gi brukere tilgang til tjenester eksternt og fra mobile enheter med tilstrekkelig informasjonssikkerhet og personvern.	R6, R12
BD3	Brukere i helseforetakene skal kommunisere med hverandre og med pasienter og pårørende med tilstrekkelig konfidensialitet, integritet og tilgjengelighet for tjenestene.	R3, R4, R6, R7, R8, R20, R21
BD4	Skytjenestene skal tilfredsstille helseforetakene i regionens sikkerhetskrav og regulatoriske krav til sikkerhet og personvern.	R15, R18, R20
BD5	Skytjenestene skal kunne driftes sikkert og kostnadseffektivt med høy grad av sentralisering og automatisering, og leverandør skal kunne byttes uten urimelige kostnader eller at data går tapt	R1, R4, R6, R16, R17, R20
BD6	Skytjenestene skal dekke krav knyttet til samhandling, dokumentdeling og videokonferanser i henhold til informasjonssikkerhetskrav gitt gjennom Helse Sør-Øst sitt ISMS.	R2, R3, R5, R15, R20, R21
BD7	SPHF må tilpasses drift av skytjenester basert på en modell der ansvar for sikkerhet er synliggjort og ivaretatt slik at ingen deler av arkitekturen er uten aktiv forvaltning.	R19, R20
BD8	Skytjenester skal være underlagt helseforetakenes styring og ettersyn (governance) i henhold til Helse Sør-Øst sitt ISMS.	R18, R19, R20
BD9	Skytjenestene skal kunne skalere i takt med behovet og være fleksible med hensyn på tjenestemodell.	R2, R5, R13, R14
BD10	Teknisk miljø for skytjenester må kunne samhandle med tjenester i eksisterende datasenter på en måte som ivaretar krav til konfidensialitet, integritet og tilgjengelighet.	R8, R9, R10, R11, R21
BD11	Skytjenestene skal kunne tilby programvareutvikling og testing, samt analyse av store datasett i henhold til informasjonssikkerhetskrav gitt gjennom Helse Sør-Øst sitt ISMS.	R9, R10, R11
BD12	Valg og håndtering av skytjenesteleverandører skal utføres slik at gjeldende informasjonssikkerhetskrav etterleves.	R15, R18, R19

7 Konseptuell sikkerhetsarkitektur

Den konseptuelle sikkerhetsarkitekturen fokuserer på foretakene i regionen sine behov og mål for informasjonssikkerhet, hvilke av regionens verdier som må sikres samt risikoer og muligheter knyttet opp mot regionens drift og kjernevirksomhet. Her defineres altså konsepter og krav i forbindelse med

bruk av skytjenester sett fra et sikkerhetsperspektiv, som setter føringer for valg og organisering av logiske og fysiske sikkerhetselementer på lavere nivå[4].



Figur 3 – Overordnet målarkitektur for IKT-infrastruktur i HSØ

7.1 Sikkerhetsledelse og ansvar

Når det gjelder informasjon, data og opplysninger[5] er det alltid dataansvarlig, HF-ene i regionen, som har det endelige ansvar for at dataene blir behandlet i henhold til gjeldende regelverk. Dette betyr at ansvaret for å etterleve regelverk ikke kan fraskrives HFene, selv om dataene behandles hos en skyleverandør. SPHF er databehandler for de øvrige HFene, og skal forvalte IKT-avtaler i regionen på vegne av HFene.

[4] Se dokumentet «Regionale sikkerhetsprinsipper for bruk av skytjenester»
[5] Herunder personopplysninger, personopplysninger av særlig kategori, virksomhetsinformasjon, konfigurasjonsdata mv.

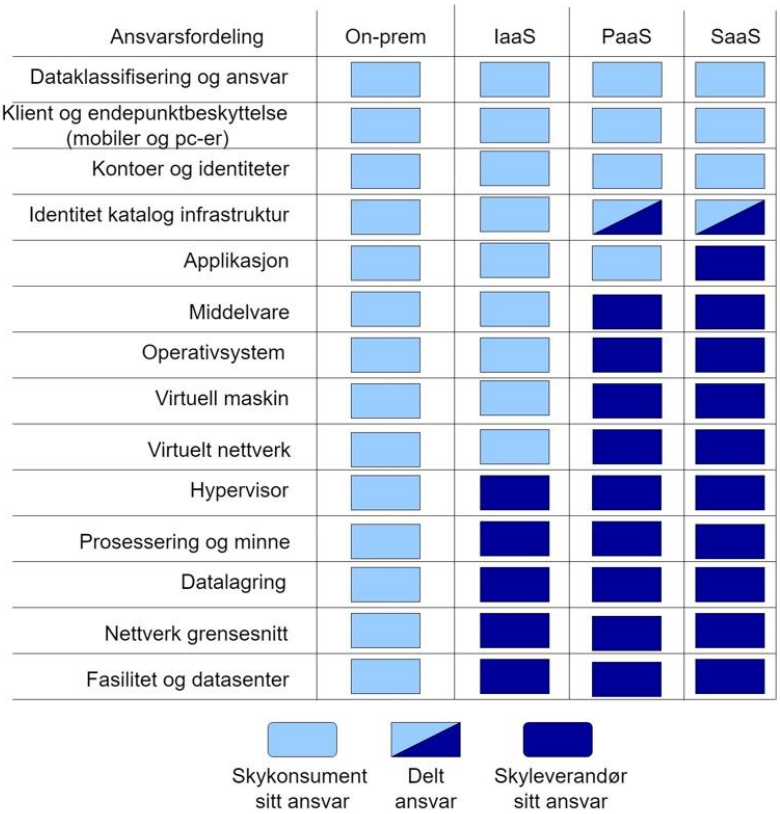
Det vil alltid være dataansvarlig sitt ansvar å klassifisere de data som er i bruk i skyløsningen. Data skal klassifiseres i henhold til gjeldende modell for informasjonsklassifisering hentet fra det Regionale ISMS. Data skal håndteres og sikres i henhold til denne klassifiseringen.

Hvem som har ansvar for beskyttelse av sluttbrukerapplikasjoner, tilgangskontroll, sikkerhet på applikasjonsnivå, nettverksnivå, og infrastruktur, kommer an på valgt tjeneste- og leveransemodell og må avklares før skytjenesten tas i bruk.

7.1.1 Ansvarsfordeling for sikkerhetstiltak

Hvordan sikkerhetsledelse og ansvar for utførelse av sikkerhetstiltak i praksis fordeles når det kommer til skytjenester, kommer an på valgt tjenestemodell. Enkelte sikringstiltak må alltid utføres av Sykehuspartner og helseforetakene selv, mens andre ivaretas av skyleverandøren. Fordeling av ansvar kontraktsfestes. Områdene Sykehuspartner og helseforetakene er ansvarlig for må det etableres rutiner for å ivareta, og utførelsen må kvalitetssikres med bl.a. risikovurdering. Områdene skyleverandøren det avtales at leverandøren er ansvarlig for må skyleverandøren utføre tilsvarende kvalitetssikring av, og kvalitetssikres av Sykehuspartner gjennom revisjon.

Skyleverandøren kan benytte underleverandører for å levere deler av tjenesten, eller til å utføre sikkerhetsoppgaver, men Sykehuspartner forholder seg alltid til parten det er inngått konkrakt med. Dette gjelder også i risikovurderinger, leverandørvedlegg, og revisjoner.



Figur 4 - Matrise for sikkerhetstiltak mellom ulike typer tjenestemodeller

Der hvor områder er delt mellom SPHF og skyleverandør (kategori 2) er det vesentlig at ansvarsfordelingen innenfor området presiseres i kontrakten slik at alle sikkerhetstiltak har en eier.

7.1.2 Intern forvaltning og kompetanse

Skytjenester krever også intern forvaltning hos Sykehuspartner. De syv horisontale nivåene i Figur 4 gir et overordnet bilde på hva slags type kompetanse SPHF må inneha for å sikre og forvalte skytjenester på en god måte. Figuren sier likevel ikke noe tydelig om hvilken mengde eller omfang av ressurser med riktig kompetanse som er nødvendig for å drifte og forvalte skytjenester på en trygg og sikker måte. Dette vil naturligvis avhenge av hvor mange, og hvor kompliserte, skytjenester som benyttes i regionen.

Valgt tjenestemodell (IaaS, PaaS eller SaaS) setter føringer for hva som er Sykehuspartners utøvende ansvar, hva som er leverandørens utøvende ansvar og hva som er delt utøvende ansvar mellom Sykehuspartner og leverandør, med hensyn til sikkerhetstiltak. I de tilfeller hvor Sykehuspartner har et utøvende ansvar, eller der det utøvende ansvaret er delt mellom Sykehuspartner og leverandør, må det foreligge intern kompetanse og forvaltning i henhold til type og mengde ansvar hos Sykehuspartner.

Med referanse til hva som kreves av avtaleinngåelse og –forvaltning er det også en forutsetning at Sykehuspartner innehar nødvendig juridiske ressurser, samt tilstrekkelig ressurser og kompetanse for ivaretagelse av avtaleverk på lang sikt. Figur 4 viser også behov for intern kompetanse av teknisk karakter, samt innen identitets- og tilgangsstyring og sikkerhet.

Berørte forretningsdrivere: BD7

7.2 Leverandørhåndtering

7.2.1 Risikovurdering av leverandører

Bruk av skytjenester krever at den dataansvarlige gjør dekkende risikovurderinger, og ellers følger kravene til avtaler og leverandøroppfølging i blant annet Normen. Sykehuspartner HF utarbeider risikovurderinger på vegne av de andre foretakene i regionen i henhold til etablert rutine og praksis. Det enkelte helseforetak står endelig ansvarlig for risikoaksept med bakgrunn i utarbeidet risikovurdering. Risikovurderinger som Sykehuspartner HF utarbeider på vegne av ett eller flere andre foretak i regionen skal som minimum inneholde beskrivelse av at[6]

- ansvarsfordelingen mellom dataansvarlig og databehandler er avklart, og tilpasset tjeneste- og leveransemodellen som benyttes
- dataansvarlig har oversikt over hvor data behandles geografisk
- databehandlers personell arbeider innenfor EU/EØS området.
- dataansvarlig påser at skyleverandørens eventuelle standardavtaler ikke er i motstrid med lovbestemte krav og Normens krav
- Dataansvarliges plan for ivaretakelse av informasjonssikkerhet og personvern ved avslutning av skytjenesten

Se også kapittel 7.2.2 til 7.2.4 for SLA og databehandleravtaler, 7.3 Risikostyring/risikovurdering, 7.4.3 for detaljer rundt databehandlingens lokasjon og **Feil! Fant ikke referansekilden. Feil! Fant ikke referansekilden.**.

Berørte forretningsdrivere: BD5, BD12

[6] Norm for informasjonssikkerhet kapittel 3

7.2.2 Avtaler og kontrakter

Gitt at skytjenester er en standardisert tjeneste så reguleres ansvarsfordelingen og forholdet mellom en kunde og skyleverandør gjennom en kontrakt. Som hovedregel vil en skyleverandør være den som stiller med standardiserte kontrakter og avtaleverk, dette være seg databehandleravtaler, tjeneste- og serviceavtaler (SLA) mv. Dette betyr at kvalitetssikring av kontrakten mellom kunde og leverandør av en skytjeneste er særdeles viktig. Rettigheter knyttet til styring og ettersyn av data må også gjelde skytjenester, noe som sikres gjennom avtaler med leverandør.

SPHF skal vurdere skyleverandører SPHF inngår kontrakter med. Ved å inngå avtaler med SPHF påtar leverandøren seg plikten til å pålegge sine underleverandører tilsvarende forpliktelser som skyleverandøren selv har påtatt seg ovenfor SPHF. Dette innebærer bl.a. at leverandør gjennomfører leverandørvurderinger av sine underleverandører og gjennomfører landvurderinger av land som er relevante for tjenesten. SPHF har rett til å revidere skyleverandøren for å kvalitetssikre at parten faktisk har utført sine oppgaver og forpliktelser.

Berørte forretningsdrivere: BD8, BD12

7.2.3 Tjenesteleveranseavtaler (SLA)

I alle tilfeller hvor skytjenester skal benyttes må det inngås avtaler mellom kunde og leverandør. Skytjenester er i stor grad en standardisert tjeneste med hensyn til avtaleverk og tilpasses aldri eller sjelden til den enkelte kundes ønsker eller behov.

Alle skyleverandører skal realisere tilgang til informasjonssystemer gjennom godkjente og dokumenterte løsninger. Leverandørtilgang skal ivareta krav til revisjonsspor og uavviselighet.

Tjenestene som skal leveres av en skyleverandører skal formaliseres i SLA-avtaler, som skal inkludere relevante sikkerhetskrav og ansvar for risiko og risikoreduserende tiltak (se kapittel 7.3).

Berørte forretningsdrivere: BD1, BD5, BD12

7.2.4 Databehandleravtaler og behandling av virksomhetssensitive opplysninger

I de tilfellene hvor leverandør behandler person- eller virksomhetssensitive opplysninger, skal behandlingen være underlagt avtale mellom gjeldende HF (i de fleste tilfeller SPHF) og skyleverandøren. Avtalen skal inngås gjennom egen databehandleravtale, eller så skal kravene til avtale med databehandler ivaretas av andre avtaler eller rettslige dokumenter. Avtalene må også dekke kjeden av eventuelle underleverandører.

Der mulig skal en integrator, eller skyleverandør, underskrive sikkerhetsinstruks eller så må dette søkes ivaretatt gjennom kontrakt som inngås for tjenesten (Non-Disclosure Agreement eller tilsvarende). Der det er relevant skal ansatte hos integratoren, eller skyleverandøren, signere taushetserklæring med gjeldende HF.

SPHF inngår databehandleravtaler som er i samsvar med norsk lovgiving, lever opp til GDPRs minimumskrav og ivaretar krav fra Normen[7]. Det skal fremkomme av databehandleravtalen eller kontrakt i hvilke(t) land data kan lagres og hvilke land data kan aksesseres fra. SPHF skal alltid kunne kreve innsyn i og måling av hvorvidt leverandørs sikkerhetskrav etterleves, se kapittel 7.5 Revisjon for ytterligere spesifikasjoner rundt dette.

Berørte forretningsdrivere: BD4, BD12

[7] Se spesielt krav 5.7.8 og 5.7.9

7.3 Risikostyring/risikovurdering

Risikovurdering gjennomføres ved alle endringer som kan ha betydning for informasjonssikkerheten, herunder også anskaffelser, implementering/installering, konfigurasjonsendringer og utfasing av systemer relatert til skytjenester. All ny, eller endring i, behandling av helse- og personopplysninger skal også risikovurderes.

Når bruk av skytjenester skal risikovurderes må man se til ansvarsfordelingen mellom SPHF og skyleverandør og hvilken tjeneste - og leveransemodell man velger (se kapittel 7.1.1, Figur 4). Valg av tjeneste- og leveransemodell påvirker handlingsrommet for å håndtere risiko og må vurderes ved bruk av skytjenester.

Basert på tjeneste- og leveransemodell vil gjennomføringen av noen risikoreduserende tiltak treffe skyleverandøren, mens andre treffer HFene i regionen (ref kap7.1.1).

Dataansvarlig vil alltid eie risikoene ved bruk av skytjenester. Håndteringen av risikoreduserende tiltak kan overføres til skyleverandøren.

Risikovurderinger skal gjennomføres i henhold til Sykehuspartners risikovurderingsmetodikk. Utøvende ansvar for å følge opp tiltak fra risikovurderinger tildeles henholdsvis leverandør eller SPHF i henhold til valgt tjenestemodell ref. (Figur 4). For eksempel vil risikoreduserende tiltak på applikasjonsnivå i en IaaS treffe SPHF, mens det i en SaaS vil treffe leverandøren (Figur 4).

Berørte forretningsdrivere: BD1, BD12

7.4 Personvern

Helse- og personopplysninger i skyen skal behandles i tråd med gjeldende lovkrav og øvrig styrende dokumentasjon i Helse Sør-Øst. Skyleverandører vil ha rollen som databehandlere og vil ha selvstendige plikter etter personvernlovgivningen. Skyleverandører skal kun behandle personopplysninger etter instruks fra dataansvarlig.

Berørte forretningsdrivere: BD1, BD4

7.4.1 Innebygd personvern

Innebygd personvern er et sentralt krav i personvernforordningen. I forbindelse med skytjenester betyr dette at den dataansvarlige skal sørge for å velge en leverandør som er i stand til å levere skytjenester som hjelper den dataansvarlige med å etterleve personvernprinsippene.

7.4.2 Personvernkonsekvensvurdering

I enkelte tilfeller skal det gjennomføres personvernkonsekvensvurdering (DPIA) [8]. Bruk av skytjenester kan være behandlinger av personopplysninger som utløser krav om gjennomføring av DPIA. Eksempler (ikke uttømmende) på tilfeller det det må gjennomføres DPIA er:

- Når skytjenester benyttes til å behandle genetiske opplysninger om store mengder mennesker
- Når skytjenester benyttes sammen med «innovativ teknologi», som velferdsteknologi
- Når skytjenester benyttes til systematisk monitorering av personer
- Når skytjenester benyttes til å behandle lokasjonsopplysninger
- Når skytjenester benytter personopplysninger til å trene kunstig intelligens

[8] Datatilsynet - Når må man gjennomføre en vurdering av personvernkonsekvenser?

Alle foretak i regionen har et personvernombud. Vedkommende kan rådføres når det gjelder personvernkonsekvensvurderinger mv.

7.4.3 Behandlingens lokasjon

Når helseforetak benytter skyløsninger til å behandle personopplysninger, skal den geografiske lokasjonen der behandlingen skjer være kjent og skriftlig dokumentert. Den dataansvarlige skal ha tilgang til dokumentasjonen av hvor behandlingen skjer.

SPHF skal kun benytte leverandører som kan garantere tilfredsstillende garantier for de registrertes personvern. SPHF skal tilstrebe å benytte leverandører som er registrert i EU/EØS-området (inkludert Norge), og følger regelverket her. Behandling av personopplysninger hos leverandører som er registrert utenfor EU/EØS er likevel tillatt når ett av vilkårene nedenfor er oppfylt:

- Behandlingen av personopplysninger skjer i en stat som Europakommisjonen har funnet til å ha tilstrekkelig vernenivå[9]
- Behandlingen skjer av et selskap som har tatt EUs standardpersonvernbestemmelser (Standard Contractual Clauses) inn i sin avtale med dataansvarlig
- Behandlingen skjer på bakgrunn av Binding Corporate Rules (BCR) hvor selskapet er etablert i EU/EØS og innenfor sitt konglomerat overfører personopplysninger ut av EU/EØS. BCR må være godkjent av kompetent tilsynsmyndighet.

I tillegg må personvernet være tilstrekkelig ivaretatt i overføringen av personopplysninger, og dette må kvalitetssikres.

Behandlinger av personopplysninger i tredjestat (dvs. stat utenfor EU/EØS) er heftet med risiko og usikkerhet. Det er muligheter for at alle de tre vilkårene for behandlinger av personopplysninger i tredjestater kan bortfalle og gjøre behandlingen lovstridig. Ved enhver behandling i tredjestater bør det derfor planlegges alternative modeller.

I tillegg til vilkårene ovenfor, må det vurderes om behandlingen av personopplysninger skjer i tråd med PSTs trusselvurderinger. Behandlinger av personopplysninger i stater der PST anser etterretningsrisikoen som høy bør unngås.

7.4.4 Segmentering av data

Skyleverandøren skal ha tekniske mekanismer som sikrer tilfredsstillende skille mellom data fra ulike dataansvarlige i skyleverandørens tekniske infrastruktur. De tekniske mekanismene skal være dokumentert. Feil på teknisk oppsett eller andre brudd på personopplysningssikkerheten som berører én av skyleverandørens kunder, for eksempel feil tilgangsstyring, skal ikke kunne ha negative konsekvenser for leverandørens øvrige kunder.

7.5 Revisjon

Det må være tydelig hvilke krav det aktuelle helseforetaket skal etterleve før bruk av skytjenester innføres. Dette slik at helseforetakene vet at attestasjoner fra leverandør og revisjoner som skal måle etterlevelse dekker relevante krav.

[9] EU's Adequacy decisions

For å vise etterlevelse eller påpeke mangler mot gitte krav relatert til informasjonssikkerhet og personvern i forskrift, standarder, policyer eller rutiner skal det gjennomføres revisjoner av skyleverandøren og tilbudte tjenester.

Revisjon av skyleverandører kan gjennomføres på følgende måter:

- Leverandøren gjør en internrevisjon, hvor leverandøren selvdeklarerer etterlevelse til visse prinsipper
- En uavhengig tredjepart kan gjennomføre revisjon av skyleverandøren (på bestilling fra helseforetaket)
- Helseforetaket utfører selv revisjon av skyleverandøren. Dette er derimot uvanlig, gitt hvordan sky-teknologi fungerer.

I tilfeller hvor uavhengig tredjepart eller helseforetaket selv skal utføre revisjon, må det påregnes en økonomisk kostnad knyttet til dette, og det er viktig at muligheten for revisjon kontraktsfestes med skyleverandøren. Valgt tjeneste- og leveransemodell innen skytjenester kan påvirke hvordan revisjoner av skyleverandører kan gjennomføres.

Revisjoner gir kun et bilde av nåsituasjonen, og de relativt raske endringene og utviklingen av teknologi og tjenestetilbud innenfor skytjenester. Dette fordrer at det må legges opp til høy frekvens av revisjoner for å følge utviklingen.

Revisjon av skytjenester bør inngå i Sykehuspartners planverk og revisjonshjul.

Berørte forretningsdrivere: BD1, BD4, BD7

7.6 Klassifisering av informasjon

Det vil alltid være respektive HF (informasjonseier/dataansvarlig) sitt ansvar å klassifisere de data som er i bruk i skyløsningen. Data skal klassifiseres etter gjeldende modell for informasjonsklassifisering hentet fra det Regionale ISMS. Data skal håndteres og sikres i henhold til denne klassifiseringen.

Berørte forretningsdrivere: BD1, BD4

7.7 Tilgangsstyring (IAM)

Tilgangsstyring til skytjenester skal etableres i henhold til målarkitektur for Identity and Access Management (IAM). Tilgang til skytjenester skal bare gis til brukere med tjenstlig behov.

7.7.1 Autorisering og autentisering

Det ligger i en skytjenestes natur at tilgangsstyring må administreres både av Sykehuspartner og av skyleverandøren. Tilgangsstyringen ved bruk av skytjenester kan kompliseres ytterligere ved at flere skytjenester og –leverandører benyttes. Krav til tilgangsstyring gjelder likt for lokale informasjonssystemer som for informasjonssystemer basert på en skytjeneste. Tilgangsstyring for skytjenester skal baseres på gjeldende prosesser i Sykehuspartner HF og benytte samme autorative kilde som lokale tjenester.

Alle brukere skal være underlagt en prosedyre som kan verifisere at en bruker er en autentisk eier av en identitet.

Skytjenester skal bare tillate handlinger som er eksplisitt godkjent. De forskjellige brukergruppene som skal benytte skytjenester har forskjellige autorisasjoner som er gitt av administratorer. Det er mange interessenter med ulike tilgangsbehov på tvers av skytjenestene og det kreves derfor en finkornet autorisasjonsmekanisme for å gi alle brukere autorisasjoner i henhold til forretningsbehov.

Tilgang til skytjenester skal bare gis til autentiserte og autoriserte brukere. Sykehuspartner skal ha rutiner for autorisering, endring og avslutning av tilganger til og i skytjenester. Federering mot eksterne autentiseringstjenester skal benyttes for eksterne brukere slik at man unngår vedlikehold av disse brukerne i Sykehuspartner. Tilgang på tvers av juridiske enheter skal sikre sømløs samhandling, og identitet og tilhørende attributter skal fødereres på tvers av HF/eksterne virksomheter.

Når skytjenester benyttes skal eksisterende tilgangsstyring, så langt det lar seg gjøre, også benyttes for tilgangshåndtering i sky. Tilganger i skyen som ikke er knyttet til en intern tilgang bør minimeres.

Berørte forretningsdrivere: BD1, BD2, BD3, BD4, BD6

7.7.2 Separation of duties

Roller og rettigheter skal være tilstrekkelig finkornet slik at (administrative) brukere aldri har flere rettigheter enn de har tjenstlig behov for. Dette gjelder både på infrastruktur- og applikasjonsnivå.

Berørte forretningsdrivere: BD4, BD7

7.7.3 Administrative/privilegerte tilganger

Administrative brukere i skyen har utvidet ansvar og myndighet og det er viktig å redusere faren for misbruk av identiteter med utvidede rettigheter. Bruker med administratortilganger skal benytte personlig separat brukerkonto for administratoroppgaver. Driftspersonell skal ha personlige brukerkontoer for oppgaver som ikke krever administratortilganger.

Risikovurdering skal begrunne behovet for ulike administratorbrukere, også administratorbrukere lokalt for skytjenesten.

Berørte forretningsdrivere: BD1, BD4, BD7

7.7.4 Kontroll av tilganger

Det skal gjøres kontroll av tilganger til skytjenester på lik linje med kontroll av andre tilganger i Sykehuspartner HF.

Berørte forretningsdrivere: BD1, BD4.

7.8 Fysisk sikkerhet/adgangskontroll

Det respektive helseforetak i regionen er endelig ansvarlig for sine data (dataansvarlig) som lagres i sky.

Ved bruk av skytjenester er skyleverandør helt og fullt utøvende ansvarlig for fysisk sikring og adgangskontroll til sine anlegg. Grad av fysisk sikring må reguleres gjennom avtaler med skyleverandør.

Sykehuspartner, på vegne av foretakene i regionen, må derfor be leverandøren fremskaffe dokumentasjon på at tiltak knyttet til fysisk sikring er i henhold til gjeldende lovverk[10] og nasjonale føringer og anbefalinger.

Berørte forretningsdrivere: BD12

7.9 Monitorering, logging og deteksjon

Monitorering, logging og deteksjon i forbindelse med skytjenester skal integreres i Sykehuspartners eksisterende regime for dette. Hvordan dette oppnås er i noen grad avhengig av hvilken tjenestemodell som benyttes[11] og hva leverandør tilbyr av data.

Det vil være nødvendig å tilpasse og videreutvikle Sykehuspartners evne til å drive tilstrekkelig monitorering, logging og deteksjon i forbindelse med skytjenester.

Behandling av helse- og personopplysninger skal logges i henhold til gjeldende lovkrav.

Viktige informasjonssikkerhetshendelser, for eksempel intrusjonsforsøk, må detekteres og rapporteres umiddelbart slik at angrep kan begrenses og stoppes.
Berørte forretningsdrivere: BD1, BD4, BD5

7.10 Hendelseshåndtering og etterforskning

Med bakgrunn i skytjenesters flyktighet og fleksibilitet som kan gi store endringer i raskt tempo vil hendelseshåndtering og etterforskning i større grad fordre automatisering.

Hendelseshåndtering og etterforskning i skytjenester må planlegges og beskrives i Sykehuspartners beredskapsplan, og videre avtales med den enkelte leverandør i SLA med hensyn til hendelseshåndteringsprosessen.

Det er viktig at skyleverandøren har ett kontaktpunkt i regionen når det gjelder sikkerhetshendelser. Tjenesteansvarlig for den enkelte skytjeneste må sørge for at skyleverandøren har en kommunikasjonskanal mot regionens Computer Emergency Response Team (CERT), slik at hendelser, sårbarheter, trusler og etterforskning kan varsles. Slike kommunikasjonskanaler må dokumenteres i Sykehuspartners beredskapsplanverk.

Leverandør av skytjenester skal uten ugrunnet opphold varsle Sykehuspartner CERT i henhold til avtalte rutiner om sikkerhetsavvik som må håndteres.

Berørte forretningsdrivere: BD4, BD7

7.11 Trussel- og sårbarhetshåndtering

Trusler mot, og sårbarheter i, infrastruktur eller nettverk i en skytjeneste håndteres hovedsakelig av skyleverandøren selv[12]. Dette kan håndteres ulikt fra leverandør til leverandør. SPHF må i denne sammenheng etterspørre dokumentasjon fra skyleverandør knyttet til utførte sikkerhetsrevisjoner og sertifiseringer med hensyn til trussel- og sårbarhetshåndtering.

[10] Herunder Sikkerhetsloven, samt veiledninger og retningslinjer fra Nasjonal Sikkerhetsmyndighet, eventuelt tilsvarende lovverk i den aktuelle stat.
[11] Tilgang til logger og loggtyper er oftest mer tilgjengelig for dataansvarlig ved bruk av IaaS og PaaS, og i mindre grad ved SaaS.
[12] Unntaket gjelder for IaaS-tjenester. Mer om dette i regionale sikkerhetsprinsipper for bruk av skytjenester

Både driftspersonells personlige sertifiseringer og leverandørsertifiseringer er informasjon som skal innsamles for å vurdere en leverandørs modenhet med tanke på operasjonell sikkerhet.

Sikkerhetskonfigurasjon for IKT-utstyr i skytjenesten skal være dokumentert og tilgjengelig for Sykehuspartner som leverandør av IKT-tjenester til helseforetak i regionen. Skyleverandør skal ha en sporbar endringskontroll på konfigurasjon av IKT-utstyr og systemer.

Berørte forretningsdrivere: BD1, BD4, BD5, BD7, BD8, BD10, BD12.

7.12 Endringshåndtering

Med hensyn til Normen kap. 5.4.2[13] skal alle HF ha et regime for endringshåndtering. Dette gjelder også for skytjenester. Alle tjenester som tas i bruk i skyen må følge gjeldende prosess for endringshåndtering. Dette omfatter også tjenester i skyen levert etter SaaS, PaaS eller IaaS modellene. Det er derimot viktig å merke seg at skyleverandøren selv har et eget endringshåndteringssystem, og at disse ikke nødvendigvis er kompatible med foretakets system. Det er derfor viktig at det opprettes en kommunikasjonskanal mellom Sykehuspartner HF og skyleverandør, slik at endringshåndtering hos skyleverandøren kan synkroniseres, eller hensyntas, hos relevant HF. Dette er viktig for å sikre en uavhengig kvalitetssikring og vurdering av risikoer, samt sikre nødvendig tilgjengelighet.

Berørte forretningsdrivere: BD1, BD5, BD7

7.13 Business Continuity, tilgjengelighet og oppetid

Alle skytjenester skal klassifiseres basert på tilgjengelighetskrav. Kravene skal spesifiseres i tjenestebeskrivelsen og er viktig fordi alle tjenester ikke trenger å ha samme krav til kontinuitet. Krav til tilgjengelighet og oppetid trenger ikke vurderes annerledes for skytjenester enn for interne tjenester og infrastruktur.

Når det kommer til forretningskontinuitet, tilgjengelighet og oppetid er det viktig å etablere hva som er det enkelte HFs ansvar og hva som er skytjenesteleverandørens ansvar.

Det enkelte HF har ansvar for å etablere og vedlikeholde beredskapsplaner (disaster recovery og business continuity). Sett opp mot skytjenester må disse dekke[14]:

- Ansvar og vaktordninger for håndtering av hendelser hos gjeldende HF
- Effektiv håndtering gjennom godkjente og kjente retningslinjer, instrukser, prosedyrer og prosesser
- Varslingsrutiner internt i HFet, samt varsling mot relevante leverandører og andre interessenter
- Kontinuitetsplanverk, inkludert for hver skytjenesteleverandør
- Prioriteringsliste over informasjonssystemer, inkludert skytjenester
- Årlige beredskapsøvelser, gjerne inkludert for skytjenester og involvering av leverandør

I avtaler mellom Sykehuspartner HF, som regional IKT-leverandør, og skytjenesteleverandøren må det være klart hva varslingsrutiner er og hvem som har ansvar for hva når det kommer til kontinuitet og gjenoppretting av skytjenester, dersom noe skjer på HFet eller skytjenesteleverandørens side.

[13] Normen punkt 5.4.2
[14] Helse Sør-Øst Sikkerhetsstrategi punkt 4.2.27

Tjenester skal være overvåket for bortfall av hele eller deler av tjenesten. Skytjenesteleverandøren har også et ansvar for vaktordning for håndtering av hendelser internt hos seg, og for at de holder seg oppdaterte og forberedte gjennom beredskapsøvelser.

Det er viktig at en skytjenesteleverandørs kapabilitet til å levere sikre og stabile tjenester tas med som et element i risikovurderingen av nye tjenester og leverandører.

Informasjon som legges i skyen skal være enkelt tilgjengelig for brukere, både fra mobile og stasjonære enheter.

Skytjenestene må kunne tilbakeføres til operasjonell status etter sammenbrudd eller annen hendelse som medfører driftsstans i henhold til SLA.

Berørte forretningsdrivere (tilgjengelighet): BD1, BD2, BD3
Berørte forretningsdrivere (oppetid): BD1, BD5

7.14 Datasikkerhet og -livssyklushåndtering

Datasikkerhet er viktig også når skytjenester benyttes, og alle former for cyberkriminalitet må forebygges. Bruk av skytjenester skal beskyttes mot ondsinnede handlinger og angrep både internt og eksternt fra over nettverk via nettverksperimeter. Prinsipper for zero-trust må gjelde også for skytjenester.

Alle sikringstiltak også for skytjenester skal være risikobaserte, slik at ikke alle tjenester, systemer og informasjon beskyttes likt. Når det kommer til bruk av skytjenester er det viktig at det finnes en oversikt over:

- Hvilke data som går til skyen og hvor, data må sikres både under overføring til og når den er lagret i skyen
- Beskytte og administrere data i skyen
    - Tilgangskontroll (se kapittel 7.7)
    - Kryptering (se kapittel 7.15)
    - Arkitektur (se kapittel 7.18)
    - Monitorering (se kapittel 7.9)
    - Tilleggskontroller relatert til spesifikk leverandør samt tjeneste- og leveransemodell
- Håndtering av livssyklus for datasikkerhet og informasjon
    - Styring og etterlevelse
    - Backup og forretningskontinuitet, tilgjengelighet og oppetid

Det må sikres at eksisterende policyer rundt livssyklushåndtering for sikring av data også gjelder i skyen. Dette inkluderer regler og prinsipper for etablering og oppdatering, lagring, bruk, deling, arkivering og sletting av data i sky. Datasikkerhetslivssyklus håndteres gjennom kontraktuelle tiltak og sikkerhetskontroller. Alle tjenester som tas i bruk i skyen må følge gjeldende prosess for service asset & configuration management[15].

Berørte forretningsdrivere: BD1, BD4, BD6

[15] Service Asset and Configuration Management

7.15 Kryptering og nøkkelhåndtering

Med hensyn til kryptering av data følger Helse Sør-Øst anbefalinger gitt av Nasjonal Sikkerhetsmyndighet (NSM).

Kryptografiske kontroller for bruk av skytjenester må implementeres i de tilfeller dette fremkommer som nødvendig på bakgrunn av en risikovurdering. De kryptografiske kontrollene skal være sterke nok til å mitigere de risikoer som er identifisert. Hvordan kryptering og nøkkelhåndtering gjøres i praksis for skytjenester, vil avhenge av valgt leverandør og valgt tjeneste- og leveransemodell. IaaS, PaaS og SaaS gir ulike krypteringsmuligheter, og valgt krypteringsløsning må gjøres på bakgrunn av gjeldende trusselbilde og tekniske og forretningsmessige krav. Løsning for nøkkelhåndtering må velges ut fra krav til effektivitet, tilgjengelighet, forsinkelse og sikkerhet.

SPHF skal ansvarliggjøre skyleverandør når det kommer til kryptering og nøkkelhåndtering.

SPHF skal stille krav til skyleverandør slik at infrastrukturen som benyttes, samt de kryptografiske algoritmene, er i samsvar med:

- Internasjonalt/nasjonalt lovverk
- Nasjonale føringer
- Regionale føringer og anbefalinger

Den nasjonale tilsynsmyndigheten for tillitstjenester er Nasjonal kommunikasjonsmyndighet (NKOM), og deres liste over kvalifiserte tillitstjenester kan sees til hvis tjenesten skal behandle person- og helseopplysninger. Skyleverandørens sertifiseringer mht. kryptering og nøkkelhåndtering skal dokumenteres.

Berørte forretningsdrivere: BD1, BD2, BD3

7.16 Mobilsikkerhet

Skyleverandørens bruk av mobile enheter for administrasjon, drift eller vedlikehold av sine tjenester skal dokumenteres, og skyleverandøren skal dokumentere at nødvendige sikkerhetstiltak for sine mobile enheter er implementert.

Informasjonen på en mobil klient skal som minimum sikres like godt som ved bruk av en ordinær klient, men på grunn av økt risiko ved tap av enhet under transport eller lignende, må det som minimum[16]:

- vurderes om tiltak for å redusere sannsynlighet for informasjonstap må implementeres
- følge prinsipp om at personopplysninger ikke lagres på mobilt ukryptert medium

Bruk eller innføring av mobile enheter skal alltid risikovurderes, og konsekvenser for personvernet må vurderes.

Berørte forretningsdrivere: BD2

7.17 Human Resource-sikkerhet

Det er viktig å sikre at ansatte hos skytjenesteleverandøren forstår sin rolle og sitt ansvar og har kompetansen de trenger til å utføre sine arbeidsoppgaver slik at risikoen for (menneskelige) feil minimeres. Skytjenesteleverandøren skal kunne dokumentere hvordan de driver opplæring når det

[16] Helse Sør-Øst Sikkerhetsstrategi punkt 4.2.26

kommer til sikkerhet, og hvordan personell opprettholder sin kompetanse.

Skyleverandøren skal forholde seg til følgende:

- Awareness/opplæring
    - Alle ansatte hos skytjenesteleverandøren skal få opplæring i informasjonssikkerhet, tilpasset den enkelte rollen. Skytjenesteleverandøren skal ha et dokumentert opplæringsprogram som de ansatte oppdateres på jevnlig.
- Sikkerhetsinstruks/taushetserklæring/NDA
    - Der mulig skal ansatte hos en skyleverandør underskrive sikkerhetsinstruks, ellers må dette søkes ivaretatt gjennom kontrakt som inngås for tjenesten (Non-Disclosure Agreement eller tilsvarende). Der det er relevant skal ansatte hos skyleverandøren signere taushetserklæring med gjeldende HF.
    - Alle hos skyleverandøren som utfører arbeid for, eller arbeid i, helseforetakenes systemer, skal ha fått informasjon om og være kjent med, konsekvensene ved brudd på sikkerhetsreguleringer.
- Identifisering av leverandører[17]

Berørte forretningsdrivere: BD1, BD4, BD8, BD12

7.18 Infrastruktur og virtualisering

Infrastruktur skal deles inn i flere sikkerhetsnivåer i henhold til ny «Policy for Regional Sonemodell» og informasjonsklassifiseringsmodellen. Det skal foreligge sikkerhetskontroller som detekterer og forhindrer ikke godkjente tjenester, uønskede handlinger og eksterne trusselagenter.

Nettverkstrafikk skal overvåkes. Dette inkluderer til og fra skytjenester og leverandørtilgang, som alltid skal realiseres gjennom godkjent løsning.

Skytjenestene må kunne skalere for å håndtere økt bruk, krav til datalagring, prosesseringskapasitet med mer som kan oppstå gjennom tjenestenes levetid. Prosesseringskapasitet og lagringskapasitet må være tilgjengelig for skytjenestene når det er nødvendig. Bruk av skytjenester skal kunne utvides til å kunne supportere nye krav til sikkerhetsarkitektur og tjenester etter behov. Sikkerhetsarkitekturen må kunne utvides og skalere for å ta høyde for nye brukergrupper (interne og eksterne), klientenheter og samhandlingsmønstre.

Bruk av virtualiseringsteknologi skal følge fastlagte prinsipper i henhold til beste praksis, leverandørens anbefalinger, regionens ledelsessystem for informasjonssikkerhet, samt kontrollrammeverk som beskrevet i Regional sikkerhetspolicy for skytjenester og øvrige tilknyttede dokumenter.

Berørte forretningsdrivere: BD9

7.19 Applikasjonssikkerhet

Bruk av skyteknologi driver frem endringer og nye muligheter for utvikling av og sikkerhet i applikasjoner. Skyteknologi kan gi et bedre sikkerhetsgrunnlag, mer automatisering, isolerte miljø og –virtuelle maskiner samt elastisitet. Det gir også noen utfordringer for applikasjonssikkerhet som må vurderes, som begrenset synlighet, logging og monitorering, og endret trusselbilde. Derfor er det viktig at SPHF forstår kapasiteten til leverandør på sikkerhet, og stiller krav til at leverandør:

[17] Iht. eIDAS-forordningen

- Integrerer sikkerhet inn i applikasjonsdesign-prosessen
- Integrerer sikkerhetstesting i utviklingsprosessen
- Automatiserer sikkerhetstiltak og –kontroller
- Bruker de iboende egenskapene og mulighetene i skytjenester til å dele opp mellom produksjons- og utviklingsmiljø

Krav til applikasjonssikkerhet i sky kan trekkes ut fra CCM og CAIQ. Disse kommer i tillegg til applikasjonssikkerhetskrav som stilles for alle applikasjoner i regionalt ISMS.

Berørte forretningsdrivere: BD4, BD9, BD11.

7.20 Interoperabilitet og portabilitet

Skytjenestene skal være designet, implementert og driftet for å tilfredsstille regionens tekniske og operasjonelle standarder. Dette slik at leverandør i så liten grad som mulig benytter proprietære løsninger, filformat og lignende, all den tid det foreligger risiko for at skyleverandørens tjeneste rammes av bortfall eller andre hendelser som hindrer eller stopper tjenesteleveransen. Det er ønskelig for en dataansvarlig å ha mulighet til å flytte hele løsninger til annen leverandør relativt sømløst. Dette er viktig for å ivareta det respektive helseforetaks eierskap til dataene og slippe avhengighet til proprietære løsninger hvor leverandøren eksempelvis kan rammes av konkurs eller oppkjøp.

I henhold til personopplysningsloven og personvernforordningen[18] har den registrerte rett til dataportabilitet – altså at data kan flyttes fra en leverandør eller et system over til en annen, og at dataene er lesbare både hos gammel og ny leverandør.

Skytjenester skal kunne samhandle med tjenester i eget datasenter slik at alle krav til sikkerhet er ivaretatt. Dette gjelder tilgang til tjenester internt, henting av data fra API, synkronisering av data og kommunikasjonstjenester.

Berørte forretningsdrivere: BD4, BD5, BD8, BD9, BD10.

[18] Lovdata - Personvernforordningen artikkel 20