HELSE SØR-ØST

Sikkerhetsprinsipper og -krav for Identity and Access Management (IAM)

1.1 Hvordan bruke dokumentet

Sikkerhetsprinsippene for IAM kan brukes som sjekkliste sammen med et løsningsdesign i forbindelse med etablering av tjeneste, endring av tjenester, eller i forbindelse med revisjoner og internkontroll av tjenester som skal benytte IAM. Dokumentet brukes også som grunnlag ved anskaffelser av tjenester som skal benytte IAM. Dette dokumentet er støttedokument til NO-19 - Sikkerhetsprinsipper og -krav for IKT-infrastruktur og applikasjoner.

1.2 Unntak fra sikkerhetsprinsippene

Unntak fra sikkerhetsprinsippene skal dokumenteres og godkjennes av Regionalt sikkerhetsfaglig råd (RSR) eller respektive informasjonssikkerhetsleder som er berørt dersom unntak kun berører et eller noen helseforetak.

- Prinsippene for forvaltning av regionalt styringssystem for informasjonssikkerhet er omtalt i dokumentet Overordnede prinsipper for regionalt styringssystem for informasjonssikkerhet.

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

1.3 IAM og Identitetsforvaltning

Dette kapittelet gjelder kravstilling til applikasjoner som skal benytte IAM (Identity and Access Management – Identitets- og tilgangsstyring).

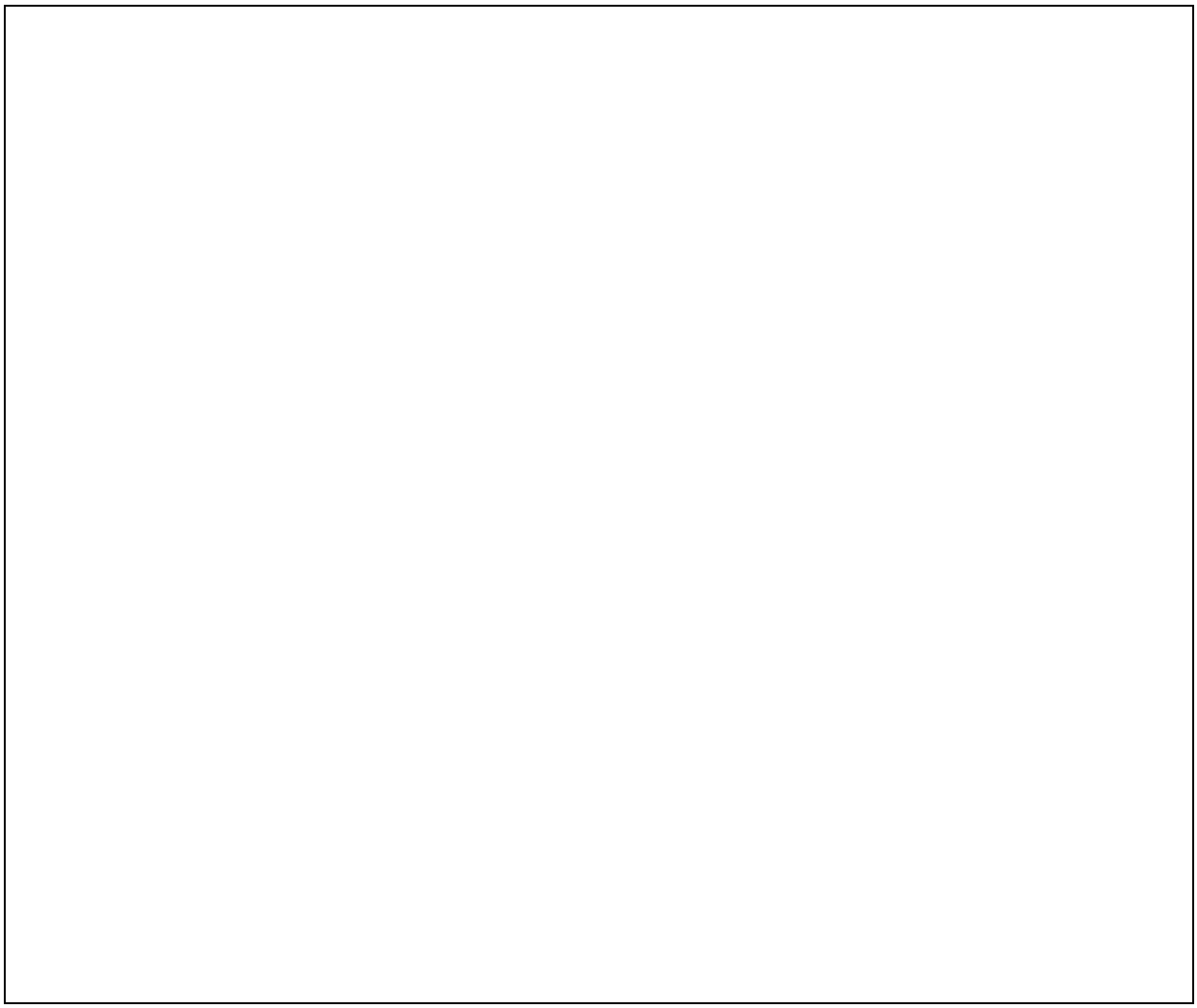
Sikkerhetsprinsipper for IAM		Etterlevd?		
		JA	NEI	I/R
8.1	Applikasjonen må støtte federering som autentiseringsmekanisme			
8.2	Applikasjonen må støtte anerkjente federeringsteknologistandarder (f.eks. SAML 2.0 eller OpenID Connect) som autentiseringsmekanisme.			
8.3	Ved bruk av SAML bør applikasjonen støtte "Service Provider initiated" federeringsprosess.			

8.4	Ved pålogging til kliniske applikasjoner må som minimum attributtene brukerid, organisasjonstilknytning og rolle tas imot og behandles for å etablere sikkerhetssesjon.			
8.5	Applikasjonen må håndheve sikkerhetssesjonen. Dette inkluderer, men er ikke begrenset til inaktivitet, start- og sluttidspunkt på token.			
8.6	Ved behov for ny eksplisitt autentisering (reautentisering og/eller autentisering av annen bruker) i en allerede etablert sikkerhetssesjon bør applikasjonens federeringfunksjon benyttes.			
8.7	Applikasjonen bør ha mulighet til å falle tilbake til alternativ autentiseringsmekanisme dersom federeringsløsning er deaktivert eller utilgjengelig.			
8.8	Ved vellykket autentisering av en bruker som ikke er autorisert til å benytte applikasjonen, skal applikasjonen ikke falle tilbake til alternativ autentiseringsmekanisme.Sluttbruker får beskjed om nektet adgang.			
8.9	Tilgang til funksjonalitet og pasientdata i applikasjonen må baseres på kombinasjon av brukers rolle og organisasjonstilknytning. I hovedsak gir rolle tilgang til funksjoner mens organisasjon styrer pasienttilgang. Dette støttes ved bruk av interne tilgangskontrollmekanismer og/eller ekstern autoriseringstjeneste.			
8.10	Applikasjonen bør spørre ekstern autoriseringstjeneste om det finnes en aktiv pasient-behandlerrelasjon dersom intern tilgangskontrollmekanisme ikke kan avgjøre tilgang.			
8.11	Dersom ekstern autoriseringstjeneste benyttes må kall mot denne gjøres iht internasjonale autoriseringsstandarder som f.eks. XACML og OAuth			
8.12	Applikasjonen må være i stand til å tilpasse seg Helse Sør-Østs sikkerhetsarkitektur relatert til attributtbasert tilgangskontroll (ABAC)			
8.13	Ved nektet tilgang bør applikasjonen presentere begrunnelsen på en forståelig måte til sluttbruker.			
8.14	Applikasjonen må støtte én entydig regional bruker-ID per person (identitet)			

8.15	Applikasjonen bør støtte gruppering av rettigheter ved at roller for tilgang kan defineres og gis rettigheter slik at brukere kan tildeles roller i stedet for individuelle rettigheter			
8.16	Applikasjonen må støtte at det kan være flere roller og/eller organisasjoner knyttet til samme entydige bruker-ID			
8.17	Applikasjonen må støtte unik identifikator for entydig identifikasjon av organisasjonsenheter.			
8.18	Leverandøren må tilpasse sitt produkt slik at tilganger kan differensieres på hvor den ansatte jobber til enhver tid			
8.19	Applikasjonen må støtte provisjonering (oppretting, lesing, endring og sletting) via standardisert programmeringsgrensesnitt (API). Programmeringsgrensesnittet må: - Være godt nok dokumentert til at en erfaren utvikler kan benytte grensesnittet uten opplæring - Ha standardisert autentiseringsmekanisme - Benytte kryptert kommunikasjon - Kommunisere over HTTP, LDAP eller SQL Programmeringsgrensesnittet bør: - Være REST-API over HTTPS tilnærmet SCIM-standarden			
8.20	APIet må muliggjøre provisjonering av påloggingsklare brukere med forhåndsdefinerte standardtilganger uten behov for manuelle tilleggsoperasjoner			
8.21	APIet bør muliggjøre tildeling av individuelle rettigheter i tillegg til standardtilganger			
8.22	Applikasjonen bør tilby et brukergrensesnitt for brukeradministrasjon, i tillegg til APIet			
8.23	APIet må muliggjøre uthenting av eksisterende data knyttet til bruker, rolle, organisasjon og tilganger fra applikasjonen			

1.4 Annet

Fyll inn annen relevant informasjon om systemet/tjenesten:



2 Definisjoner

Se eget dokument: Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet

3 Avvik eller dissens

Avvik på denne instruks meldes i virksomhetens avvikssystem. Informasjonssikkerhetsleder og/eller personvernombud skal varsles.

4 Referanser

- Se eget dokument: Sikkerhetsregulerende lovverk gjeldende for helseforetaksgruppen
- Prinsippene for anvendelse og forvaltning av dokumentet er beskrevet i dokumentet Overordnede prinsipper for regionalt styringssystem for informasjonssikkerhet.