Deklareringsområde: Informasjonssikkerhet	Versjon: 4.1 Dato: 17.08.2015

VEILEDNING OG SELVDEKLARERING FOR DELOMRÅDE:

Kravnumrene nedenfor refererer til Faktaark 38 - Sikkerhetskrav for systemer

Autorisering	Autentisering	Hendelses-registrering	Pasientrettigheter	Integritet
Kravnr. 1 til 18	Kravnr. 19 til 24	Kravnr. 25 - 31	Kravnr. 32 til 35	Kravnr. 36 til 37

1 INFORMASJON OM SELSKAP

Tabellen nedenfor bør fylles ut av leverandøren med informasjon om virksomheten og objektet.

Leverandørnavn:		
Postadresse:		
Besøksadresse:		
Organisasjonsnummer:		
Kontaktinformasjon:	***Navn på kontaktperson:***	
	E-post:	***Telefonnummer:***
Objekt:	***Benevnelse på system:***	***Hovedversjon:***
	Benevnelse delsystem:[1]	***Versjon:***
	Kommentar for å utdype beskrivelsen av objekt:	
Utfylt:	***Dato:***	***Utfylt av person:*** ☐ Samme som kontaktperson

1. *Selvdeklareringen kan være avgrenset til et bestemt delsystem. Om selvdeklareringen gjelder hele systemet med alle sine eventuelle delsystemer skal ikke hvert enkelt delsystem beskrives. I slike tilfeller angis kun systemet med en eventuelt utdypende kommentar. Eksempler på delsystem kan være: en modul i systemet, en integrasjon som hører inn under systemet og som leveres med systemet.*

2 SELVDEKLARERING AV AUTENTISERING

Med autentisering menes prosessen som gjennomføres for å bekrefte en påstått identitet. Det er flere dataelementer som inngår i denne prosessen. Disse er:

- En person har et eller flere ansettelsesforhold i virksomheten. Ansettelsesforholdet kan være arbeidsgiver/arbeidstager forhold eller at ansettelsesforholdet er etter en avtale om innleid personell
- Personen gis en unik identitet (kan være en bruker ID/brukernavn) per ansettelsesforhold
- Hver av de unike identitetene gis et unikt autentiseringskriterium (kan være passord)
- Brukeren gis en eller flere roller
- Hver av rollene har en unik rolleidentitet
- Den enkelte rolle kan ved behov gis et eget autentiseringskriterium eller benytte det samme autentiseringskriterium

Krav Nr. 19	Kravet i Normens kapittel **5.2.1** er: *Autentisering må sikre identifisering i korrekt rolle i hvert enkelt tilfelle.*
Hensikt med kravet	Hensikten med kravet er å sikre at det ikke er mulig å bli autentisert til en rolle uten at bruker er korrekt identifisert. En bruker kan ha ulike roller i virksomheten.
Veiledende beskrivelse	Systemet må ha funksjonalitet for å verifisere at brukerens oppgitte autentiseringskriterium (for eksempel passord) stemmer med rollens tilhørende autentiseringskriterium. Funksjonaliteten skal benyttes ved valg av hver enkelt rolle.
Veiledende eksempel	For eksempel kan kravet løses med at brukeren logger ut og inn av systemet og på den måten bytter bruker-ID ved bytte av rolle. Et annet eksempel på rollebytte er at bruker velger roller fra en rollemeny med roller brukeren er autorisert for.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:

Krav Nr. 20	Kravet i Normens kapittel **5.2.1** er: *Ulike roller skal identifiseres og ved behov gis ulike autentiseringskriteria.*
Hensikt med kravet	Hensikten med kravet er å sikre at hver enkelt rolle har en unik identitet og kan gis autentiseringskriteria (for eksempel passord) som er forskjellig fra andre roller.
Veiledende beskrivelse	I helse-, omsorgs- og sosialsektoren kan en og samme person ha ulike roller i samme virksomhet. Hver rolle skal ha en unik rolleidentitet. Det vil si noe i rollen som gjør den unik og forskjellig fra andre roller. ”Ved behov gis ulike autentiseringskriteria” menes at når brukeren velger den aktuelle rollen skal systemet kreve at brukeren må oppgi et annet autentiseringskriterium enn det som ble benyttet for autentisering i de øvrige rollene.
Veiledende eksempel	En metode for å identifisere den enkelte rolle kan være å gi rollen et navn etter: • stillingskategori • grupper helsepersonell etter helsepersonelloven § 48 (se http://lovdata.no/all/tl-19990702-064-009.html#48) • funksjon i virksomheten Eksempler på ”*ulike autentiseringskriteria*” er: passord, kvalifiserte sertifikater, to-faktor og biometri. Bruker kan for eksempel benytte det samme autentiseringskriterium som ble benyttet ved pålogging, for autentisering til de enkelte rollene. For å gi rollen et autentiseringskriterium som er unikt fra andre roller, kan det være en funksjon i oppsettet av rollen der dette velges.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐
Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:			

Krav Nr. 21	Kravet i Normens kapittel **5.2.1** er: *Ved tilgang til behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer skal ulike ansettelsesforhold identifiseres og gis ulike autentiseringskriteria.*
Hensikt med kravet	Hensikten med kravet er å sikre at tilgang til helse- og personopplysinger følger det enkelte ansettelsesforhold.
Veiledende beskrivelse	For veiledende beskrivelse av identifisering av ulike ansettelsesforhold vises det til veiledningsdokumentet ”deklareringsområde: autorisering”, krav 3. Systemet skal ha funksjonalitet for å etablere brukeridentiteter som kan skille mellom ulike tilknytningsforhold til virksomheten (for eksempel ansettelsesforhold og innleid personell). Om en person har flere ansettelsesforhold i virksomheten skal hver av disse gis unikt autentiseringskriterium (for eksempel brukernavn / bruker-ID).
Veiledende eksempel	Brukeridentiteten bør etableres med tilstrekkelig antall tegn slik at eventuelle begrensinger ikke medfører at ulike ansettelsesforhold ikke kan identifiseres. Systemet bør ikke ha begrensninger i antall brukerkontoer. En metode for alltid å kunne identifisere ulike ansettelsesforhold er å hindre at brukernavn /bruker-ID gjenbrukes. For å illustrere flere ansettelsesforhold kan en person har et ansettelsesforhold 3 dager i uken som fast ansatt og et ansettelsesforhold 2 dager i uken som innleid medarbeider fra en annen virksomhet. I dette tilfelle vil den samme personen ha to ansettelsesforhold. Identifisering av hvert ansettelsesforhold kan løses ved å ha funksjonalitet i systemet som muliggjør to brukeridentiteter (brukernavn) på samme bruker. En metode for å ivareta kravet kan være at skifte av ansettelsesforhold skjer ved skifte av bruker-ID.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:

Krav Nr. 22	Kravet i Normens kapittel **5.2.1** er: *Flere personer skal ikke benytte samme autentiseringskriteria.* *Utdypning av kravet der det ikke benyttes PKI:* - *Passordet skal kunne byttes enkelt av bruker* - *Tvunget skifte av passord skal være teknisk mulig* - *Passordets kvalitet og varighet skal kunne konfigureres*
Hensikt med kravet	Hensikten med kravet er å sikre at autentiseringskriteriet på den enkelte bruker faktisk er mulig å gjøre unikt. Dette innebærer at flere brukere ikke skal benytte samme bruker-ID og passord.
Veiledende beskrivelse	Dette kravet tar utgangspunkt i krav 20 som skal sikre at det er ulike autentiseringskriteria for de ulike ansettelsesforhold den enkelte personen måtte ha. Systemet må ha funksjonalitet slik at den enkelte bruker selv kan velge å bytte passord. Systemets funksjon for passordbytte bør gå intuitivt fram av skjermbildene. Funksjonen må være tilgjengelig for alle brukere av systemet. Systemet må ha funksjonalitet for tvunget skifte av passord. Konfigurasjon av denne funksjonen skal knyttes til en rolle (supervisor eller en administrator rolle). Tvunget skifte av passord skal ikke kunne overstyres av brukeren. Systemet skal ha funksjonalitet for å kunne konfigurere passordets kvalitet og varighet uten at dette kan overstyres av brukeren. Konfigurasjon av denne funksjonen skal knyttes til en rolle (supervisor eller en administrator rolle).
Veiledende eksempel	Funksjonen for bytte av passord bør gjøres enkelt tilgjengelig for eksempel i et skjermbilde for brukerens egen profil eller i menyer som er mye brukt. Funksjonen for tvungen passordbytte kan plasseres i skjermbilde for å administrere den enkelte bruker. Når bruker logger seg på systemet blir brukeren presentert for bytte av passord der bruker oppgir gammelt passord og nytt passord to ganger. Blir ikke dette godkjent avbrytes passordbytte og autentiseringen. I et skjermbilde for oppsett av brukeridentiteter kan det være en funksjon for å konfigurere passordets kvalitet og varighet. Eksempler på funksjoner for parametersetting av passordkvalitet er: - Minimum antall tegn - Krav om alfanumeriske og spesialtegning - Krav om store bokstaver - Krav om små bokstaver Tvunget passordbytte kan knyttes til en konfigurerbar tidsfunksjon. For eksempel bytte av passord hver 90.dag eller 120.dag. Følgende er eksempler på funksjoner for parametersetting av passordets varighet: - Varighet i antall dager - Antall mislykkete pålogginger før kontoen sperres

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐
Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":			

Krav Nr. 23	Kravet i Normens kapittel **5.5.2** er: *Tekniske tiltak skal iverksettes slik at personer i eller utenfor virksomheten uansett ressurser og kunnskap ikke skal kunne endre opplysninger uten at det registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystem hvem som har endret og hva som er endret.* *Utdypning av kravet der det ikke benyttes PKI:* - *Passordfil skal krypteres*
Hensikt med kravet	Hensikten med kravet er å sikre at passordet ikke kommer på avveie. Det skal kunne være mulig å hente fram informasjon om hvem som har endret helse- og personopplysninger og hva endringen består i.
Veiledende beskrivelse	Systemet må ha funksjonalitet som sikrer at passordet krypteres på en slik måte at uautoriserte ikke kan benytte det for tilgang til systemet. Med ”*hva som er endret*”, i kravet, menes at all endring av helse- og personopplysninger i systemet skal registres.
Veiledende eksempel	For eksempel kan det benyttes en hashing algoritme for å kryptere passord. På den måten lagres ikke passordet ukryptert noe sted. Systemet bør ha funksjonalitet som skjuler passordet i påloggingsbildet, skjermbilde for tvungen passordbytte eller skjermbilde der brukeren selv kan bytte passord. For eksempel kan tegnene brukeren skrive inn framkomme som ”*” - stjerner. Om passordet framkommer i ”INI-filer” eller lignende må passordet plasseres i INI-filen i kryptert form. For veiledning i kryptografi vises det til Kravspesifikasjon for PKI i offentlig sektor

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:

Krav Nr. 24	Kravet i Normens kapittel **5.5.2** er: *Alle systemer skal ha mekanismer som hindrer uautoriserte endringer av helse- og personopplysninger*
Hensikt med kravet	Hensikten med kravet er at systemet skal ha mekanismer for å kunne ivareta integriteten til helse- og personopplysninger. Når alle fem kravene nedenfor er selvdeklarert med ”Ja” eller ”Ikke relevant” vil dette kravet være selvdeklarert.
Veiledende beskrivelse	Grunnlaget for dette kravet er ivaretatt gjennom summen av kravene nedenfor: 1. Det enkelte ansettelsesforhold skal identifiseres. Se Krav Nr. 4 2. Ulike roller skal autoriseres. Se Krav Nr. 8 3. Autentiseringen skal sikre korrekt rolle. Se Krav Nr. 18 4. Ulike roller skal autentiseres og ved behov gis ulike autentiseringskriteria. Se Krav Nr. 19 5. Systemet må ha funksjonalitet som sikrer at passordet krypteres. Se Krav Nr. 22
Veiledende eksempel	Det vises til veiledende eksempel for de fem kravene som er nevnt ovenfor.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”: