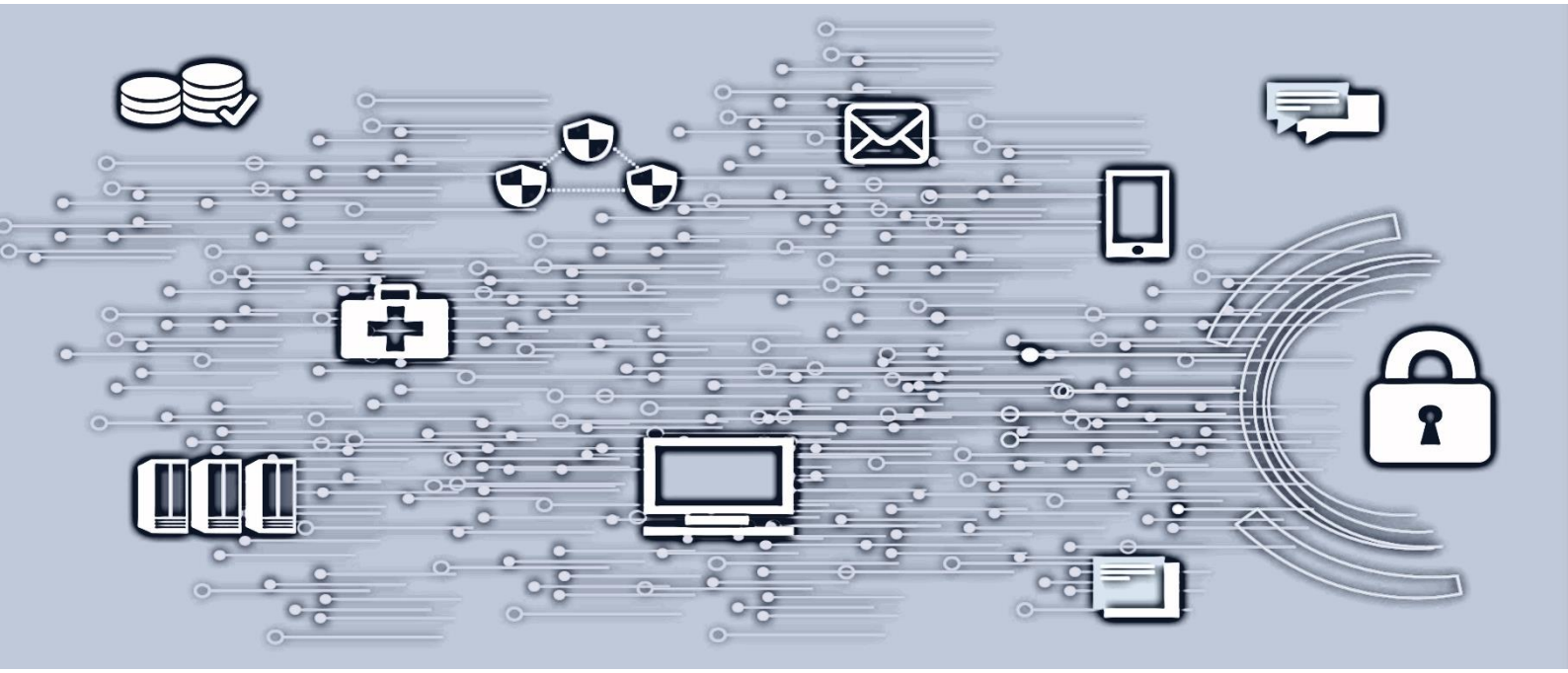
SYKEHUSPARTNER

Regional autentiseringspolicy for Helse Sør-Øst



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. Hensikt og omfang

Sikre at alle medarbeidere er kjent med kravene til autentisering for IKT-systemer i Helse Sør-Øst.

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. Regional autentiseringspolicy for helseforetakene i 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 en av sikkerhetsnivåene som benyttes i Norge og innen EU. eIDAS forordningen stiller krav til disse og tilsynsmyndigheten i Norge (NKOM) sikrer kvaliteten på metodene.

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

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

3.1 Autentiseringsmetoder og sikkerhetsnivå

Følgende autentiseringsmetoder er tillatt i Helse Sør-Øst:

Autentiseringsmetode	Sikkerhetsnivå	Godkjent av NKOM
Brukernavn og passord mot AD	Antatt nivå Lav	Nei
Mobilbasert MFA med SecurEnvoy	Antatt nivå Betydelig	Nei
Buypass PKI med lokal autoritet (kun AHUS)	Antatt nivå Betydelig	Nei
Buypass ID på smartkort	Høy	Ja
Buypass ID på mobil	Høy	Ja
Buypass ID med FIDO2	Høy	Ja
BankID	Høy	Ja

3.2 Scenarier og krav til sikkerhetsnivå

Tabellen lister de vanligste scenariene og identifisert sikkerhetsnivå på autentiseringsmetoden som benyttes. En bruker kan selv velge metode på en gitt sikkerhetsnivå om det er flere alternativer i listen over.

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 epost, 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

3.3 Krav til passord for helseforetakene i Helse Sør-Øst

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

<table>
<tr><th>Den ansattes plikter</th><th>Regionale krav til passord for helseforetakene i Helse Sør-Øst</th></tr>
<tr><td rowspan="3">- 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 mail, Facebook eller lignende)</td><td>- 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.</td></tr>
<tr><td>- 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 min
- Passordet må være forskjellig fra tidligere passord, systemet skal huske de siste 13 passordene</td></tr>
<tr><td>- Påloggінger, inkludert forsøk på feilaktig pålogging, skal logges og spores tilbake til minimum en maskinadresse</td></tr>
</table>

[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.

3.4 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 eventuelt 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

4. 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).

5. Administratorpassord i Helse Sør-Øst

Sykehuspartner HF har besluttet følgende passordkrav hvor det benyttes administratorrettigheter.

5.1 Personlige administratorpassord

Følgende krav gjelder for personlige administratorpassord:

Den ansattes plikter	Sykehuspartners regler
- 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 mail, 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 NSMs passordanbefalinger fra 2018

5.2 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	Sykehuspartners regler
- 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 mail, 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

6. 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 adminbrukere, skal sperres uten ugrunnet opphold
- Administrator skal ikke ha permanent kjennskap til ikke-individuelle passord

Det er linjeledere i Sykehusparter 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.

7. Avvik eller dissens

Avvik på denne instruks meldes i virksomhetens avvikssystem. Informasjonssikkerhetsleder og/eller personvernombud skal varsles.
Krav til sikkerhetsnivå innen autentisering er gjeldende for alle nye tjenester, men vil ikke ha tilbakevirkende kraft for eksisterende tjenester.