Fellesregional passordpolicy for helseforetakene i Helse Sør-Øst

Versjonsnummer	**Dato**	**Godkjent av**
1.0	22.12.2016	
1.1	23.10.2018	

1 Hensikt og omfang

Sikre at alle medarbeidere er kjent med kravene til passord 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, helseregisterloven og personopplysningsloven med forskrift.

- 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 Fellesregional passordpolicy for helseforetakene i Helse Sør-Øst

Alle som har et arbeidsforhold i Helse Sør-Øst tildeles en unik, personlig bruker, som identifiserer brukeren under bruk av informasjonssystemene.

Et brukernavn og et passord *autentiserer* brukeren. Autentiseringen vil gi brukeren tilgang eller *rettigheter* inn i et datasystem, avhengig av rolle, attributter eller brukeridentitet. Kravene til passord og forvaltningen av passord kan være forskjellig basert på rolle og system.

Helseforetakene i Helse Sør-Øst har kommet til enighet om følgende fellesregionale passordpolicy:

DEN ANSATTES PLIKTER	FELLES PASSORDPOLICY 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 mail, Facebook eller lignende)	- Alle brukerkontoer skal ha passord - Passordet skal bestå av minst åtte tegn - Passordet skal ha minst 3 av 5 følgende egenskaper[1]: • 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

[1] Microsoft complex password policy: https://technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx

	- Brukerkonto stenges etter 6 mislykkede påloggingsforsøk - 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

3.1 Unntak fra fellesregional passordpolicy

3.1.1 Akershus Universitetssykehus HF

Ved Akershus Universitetssykehus HF (Ahus) har man implementert løsning for bruk av tofaktorautentisering bestående av ID-kort utstedt med påloggingsserifikat for AD sammen med en kjent PIN-kode. Bruker kan velge om man bruker ID-kort + PIN-kode eller AD-brukernavn + passord når man autentiserere seg mot klient eller arbeidsflate, men ledelsen ved Ahus ønsker av sikkerhetsmessige årsaker at brukerne i størst mulig grad benytter seg av ID-kort + PIN-kode. Løsninger for Ahus blir derfor satt opp slik at det er enklest å bruke ID-kort + PIN-kode for autentisering mot klient og arbeidsflate.

For lokasjoner eller informasjonssystemer ved Ahus som ikke benytter tofaktorautentisering, eller ved brukers eget valg om å bruke AD-brukernavn + passord til autentisering gjelder den fellesregionale passordpolicy som er beskrevet i dette dokument.

3.1.2 Unntak for eldre informasjonssystemer

Flere av helseforetakene har eldre systemer eller andre typer systemer som teknisk ikke kan etterleve fellesregionale 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 fellesregional passordpolicy, eller at informasjonssystemet kan integreres med sentral autentiseringsløsning (AD), jfr. *Sikkerhetsprinsipper og krav for IKT*, punkt 7.6.1[2]

4 Administratorpassord i Sykehuspartner HF

Sykehuspartner HF har besluttet følgende passordpolicy for egen forvaltning, hvor det benyttes administratorrettigheter:

4.1 Personlige administratorpassord

Følgende krav gjelder for personlige administratorpassord

[2] SP-S-INSTRUKS-04 Instruks for bruk av passord i Sykehuspartner», versjon 1.5 pr. 2016-08-10

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 - Passordet skal ha minst 3 av 5 følgende egenskaper[3]: • 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 - Adminkonto stenges etter 6 mislykkede påloggingsforsøk - 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

4.2 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 brukerpassord 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	- Passord skal kun oppbevares i sikkert, digitalt passordhvelv.

[3] Microsoft complex password policy: https://technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx

- 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	- Passordet skal bestå av minst 16 tegn - Passordet skal ha minst 3 av 5 følgende egenskaper[4]: • 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

5 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 linjeleders om 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.

6 Definisjoner

- Microsoft complex password policy: https://technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx
- Se også dokumentet Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet

[4] Microsoft complex password policy: https://technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx

7 Avvik eller dissens

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

8 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