Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Passord og passordhåndtering

Støttedokument
Faktaark nr 31
Versjon: 2.1
Dato: 01.10.2018

Formål	Sikre konfidensialitet og integritet ved behandling av helse- og personopplysninger		
Ansvar	Sikkerhetsleder / sikkerhetskoordinator skal etablere regler slik at kravene til passord er ihht styringssystemet for informasjonssikkerhet i virksomheten.		
Gjennomføring	Regler for passordhåndtering skal etableres før behandling av helse og personopplysninger starter.		
Omfang	Omfatter alle IKT-systemer som benyttes til behandling av helse- og personopplysninger.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Leverandør ☒ IKT-ansvarlig ☐ Forsker ☐ Prosjektleder	☒ Sikkerhetsleder / sikkerhetskoordinator ☐ Virksomhetens leder/ledelse ☐ Forskningsansvarlig	☐ Medarbeider/ansatt ☒ Databehandler ☐ Personvernombud
Hjemmel	Personvernforordningen artikkel 24 og 32		
Referanser	• Norm for informasjonssikkerhet, kapittel 2.3 og 5.2.2 • Faktaark 14 – Tilgangsstyring • Faktaark 38 – Sikkerhetskrav for systemer		

Merknad 01.10.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

Nr.	Aktivitet/Beskrivelse
1	**Før passord tas i bruk (Utarbeidelse av en prosedyre for passord og passordhåndtering)** a) Krav til passordet på det enkelte system må vurderes ift: - Grad av fysisk sikring og kontroll på området der tilgangen gjøres fra - Hvilke type opplysninger som skal beskyttes - Graden av tilgang/pålogging fra eksterne nett - Graden av intern nettverkssikring i åpne og lukkede soner - Lengden, type tegn med mer på passordet må stå i forhold til bytteintervallet - Om det er tvunget bytteintervall (maskinstyrt) eller ikke b) Felles bruker-ID og passord skal ikke benyttes i applikasjoner med helse- og personopplysninger. Med felles menes at to eller flere brukere deler den samme bruker-ID og passord. c) Prosedyrene for bruker-ID og passord må inkludere: - oppretting ved ansettelser av nye medarbeidere - endring av den ansattes ansvarsområde - fratredelse/permisjon - hvem som har autorisasjon til å bestille passord og metoden dette skal skje på d) Passordprosedyrene og kravene til lengder, karakterer og bytteintervall må tilpasses det enkelte system etter hva som er mulig innenfor systemet
2	**Krav til bruk av passord** a) Utlån av passordet til andre personer er ikke tillatt b) Passordet skal ikke skrives ned slik at uautoriserte kan finne og bruke det c) Det skal være prosedyrer for hendelsesorientert bytte av passord. For eksempel om det er mistanke om at passordet er kommet på avveie eller at en risikovurdering indikerer behov for nye krav til passord

Nr.	Aktivitet/Beskrivelse
	d) Brukerkontoen må sperres eller passordet må byttes dersom det er gjort kjent for andre e) Passord skal ikke oppgis på telefon uten at det er trygghet for at det er den rette personen som får oppgitt passordet

Eksempler

Nedenfor følger eksempler på retningslinjer for passord. Den enkelte virksomhet må, med utgangspunkt i egen situasjon, sette krav til passord ut fra en risikovurdering.

Krav til vanlig bruker

- Passordet skal endres ved første gangs pålogging på det aktuelle systemet slik at det kun er brukeren som kjenner passordet
- Passordet skal være minimum 7 tegn, kombinasjon av bokstaver, tall og spesialtegn
- Samme passord skal ikke brukes om igjen i forbindelse med passordbytte
- Passordet skal ikke inneholde navn eller fødselsdato til bruker eller vedkommendes familie. Det skal ikke benyttes navn på kjæledyr, bilmerke eller annet personlig som kan knyttes til brukeren
- Passordet skal byttes hver 180. dag
- Det er ikke tillatt å skrive ned passordet på papir slik at det kan komme uautoriserte i hende
- Passordet er personlig og skal ikke deles med andre personer
- Brukeren oppfordres til å benytte samme passord på flere systemer for å forhindre at det blir for mange passord å huske
- Det bør ikke benyttes samme passord på eksterne tjenester som på interne tjenester
- Antall mislykkede påloggingsforsøk er 5 ganger før kontoen sperres

Krav til fellesbruker ved pålogging på nettet

- Fellesbruker kan benyttes til pålogging i nettet i avdelinger der flere personer benytter samme arbeidsstasjon for raskere tilgang til pålogging til applikasjoner med helse- og personopplysninger
- Fellesbruker skal benyttes unntaksvis for pålogging på nettet og etter en risikovurdering
- Passordet skal være minimum 7 tegn, kombinasjon av bokstaver, tall og spesialtegn
- Passordet skal byttes forholdsmessig ift antall medarbeidere som benytter fellesbrukeren, det fysiske området fellesbrukeren benyttes i og hyppighet i utskiftning av personell
- Det er ikke tillatt å skrive ned passordet på papir slik at det kan komme uautoriserte i hende
- Antall mislykkede påloggingsforsøk er 5 ganger før kontoen sperres

Krav til systemadministrator (nettverksutstyr, databaser, operativsystemer)

- Passordet skal være minimum 8 tegn, kombinasjon av bokstaver, tall og spesialtegn
- Samme passord skal ikke brukes om igjen i forbindelse med passordbytte
- Passordet skal ikke inneholde navn eller fødselsdato til bruker eller vedkommendes familie. Det skal ikke benyttes navn på kjæledyr, bilmerke eller annet personlig som kan knyttes til brukeren
- Passordet skal byttes hver 180. dag
- Passord skal byttes umiddelbart om det er mistanke om at uautoriserte har fått kjennskap til passordet
- Der det benyttes personlige kontoer med systemadministrative rettigheter, skal kontoene omfattes av prosedyrer/passordkrav som for systemadministratorer
- Det er ikke tillatt å skrive ned nettverkspassord(ene) i ukrypterte datafiler i nettverket. (Ref. Faktaark 38 – *Sikkerhetskrav for systemer* vedrørende krav til kryptering av passordfil)
- Antall mislykkede påloggingsforsøk er 3 ganger før kontoen sperres
- Passordet skal oppbevares i forseglet konvolutt i safe eller bankboks. Det skal føres hendelsesregister for åpning av konvolutten. Årsak, tid og navn skal dokumenteres. Alternativt benyttes passordhåndteringssystemer