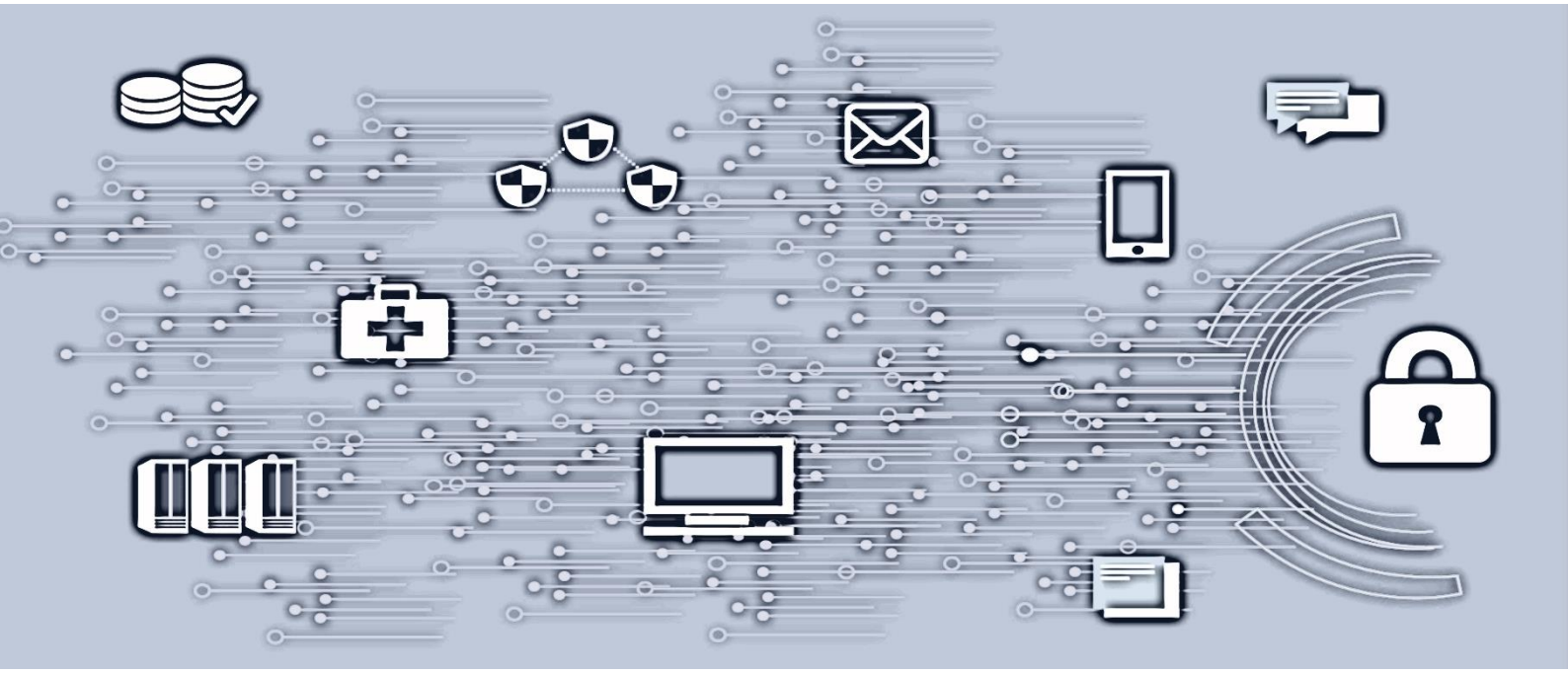
SYKEHUSPARTNER

Sikkerhetsinstruks



Innhold

Versjon	Dato	Godkjent av
1.0	2016-12-22	
1.1	2018-10-23	
1.2	2019-09-03	Øyvind Grinde
1.6	2021-08-19	Øyvind Grinde
1.7	2022-03-24	Christian Jacobsen
1.8	2022-03-14	Christian Jacobsen

1. Hensikt og omfang

Denne sikkerhetsinstruksen gjelder for alle medarbeidere, leverandører, konsulenter, vikarer og andre som gis tilgang til virksomhetens elektroniske tjenester. Dette omfatter all bruk av virksomhetens informasjonssystemer, inkludert, men ikke begrenset til, stasjonært og bærbart utstyr, nettverk, pasientsystemer og andre behandlingsrettede helseregistre, programvare, medisinsk-teknisk utstyr m.m.

Instruksen skal være lest og gjennomgått før det gis tilganger til virksomhetens elektroniske tjenester.

Virksomheten skal sørge for at instruksen er lett tilgjengelig for alle ledere og medarbeidere i virksomheten.

Enhver leder er ansvarlig for å informere om denne instruks og gjøre den tilgjengelig for sine medarbeidere.

2. Sikkerhetsinstruks

2.1 Taushetsbelagte opplysninger

Som medarbeider skal du som hovedregel kun ha tilgang til de opplysningene som er nødvendig for å kunne utføre dine arbeidsoppgaver. Det er forbudt å søke etter pasientopplysninger og annen taushetsbelagt informasjon, f.eks. informasjon om medarbeidere, familiemedlemmer og kjente personer, uten at dette er nødvendig for ditt arbeid (tjenstlig behov), at du har grunnlag for å søke opp informasjonen og at taushetsplikten herunder er ivaretatt. Brudd på taushetsplikt kan få konsekvenser for arbeidsforholdet og vil kunne medføre straffansvar.

Du skal være kjent med følgende:

- at Helse Sør-Øst forvalter taushetsbelagt informasjon, herunder opplysninger om helse og andre personlige forhold og forretningshemmeligheter.
- at dersom du gjennom utførelse av arbeid/oppdrag/tjeneste i Helse Sør-Øst får kjennskap til taushetsbelagt informasjon, forplikter du deg til ikke å bruke, utlevere eller på annen måte gjøre tilgjengelig denne kunnskap for internt eller eksternt uvedkommende og ikke benytte denne til andre formål enn de oppgaver du er pålagt av helseforetaket.
- at du plikter å gjøre deg kjent med både den forvaltningsmessige og profesjonsbaserte taushetsplikten som følger av lovverket.
- at taushetsplikten gjelder uten tidsbegrensning, med mindre medarbeider løses fra denne plikt av hvert av helseforetakene medarbeider har jobbet for i Helse Sør-Øst.
- at du plikter å overholde arbeidsgivers til enhver tid gjeldende etiske retningslinjer.
- at forsettlig eller uaktsomt brudd på taushetsplikten kan medføre disiplinære sanksjoner, erstatningsansvar og straffeansvar.

2.2 Pålogging og avlogging, brukernavn, passord og skjermsparer

Passordet (og eventuelt andre autentiseringsmetoder) er den ansattes personlige nøkkel til virksomhetens informasjonssystemer og skal ikke deles med andre. Den enkelte ansatte/innleide har et personlig ansvar for å sørge for at andre ikke får tilgang til passord e.l.

- Det er ikke tillatt å bruke en annens brukertilgang/passord.
- Passord skal ikke skrives ned.
- Ved mistanke om at passordet er blitt kjent av andre, skal passordet byttes uten ugrunnet opphold.
- Passordbeskyttet skjermsparer skal benyttes og/eller kontordør låses når arbeidsplassen/maskinen forlates i kortere perioder.
- Brukeren skal alltid logge ut sin personlige tilgang før maskinen overlates til andre.

Mer informasjon om grunnlag for oppslag i journal, finnes i dokumentet Grunnlag for oppslag i journal.

2.3 Logging

All bruk av virksomhetens informasjonssystemer kan bli loggført. Loggene brukes til administrasjon, for å følge opp virksomhetens retningslinjer for informasjonssikkerhet og for lovpålagt kontroll av oppslag i behandlingsrettede helseregistre (eks. DIPS).

2.4 Om privat bruk

Virksomhetens informasjonssystemer er beregnet for jobbrelaterte formål, og skal som hovedregel benyttes til dette.

- Noe privat bruk tillates, inkludert mindre mengder e-post, nyheter og opplysningstjenester. Dette må imidlertid ikke påvirke jobbrelaterte oppgaver, eller være i strid med denne instruks, lover eller allmenne normer for oppførsel og sosial atferd. Privat e-post som lagres skal legges i mappe merket “privat”.
- Mindre mengder private filer kan lagres i egen katalog på personlig område i sykehusnettet, forutsatt at katalogen er merket "privat". Av plass og kapasitetshensyn skal ikke private bilder, video, musikkfiler eller tilsvarende lagres i sykehusnettet.

Ansatte skal ikke bruke sin e-postadresse ved foretaket når de opptrer som privatpersoner på internett, for eksempel på sosiale nettsteder.

2.5 Bruk av Sykehuspartner-brukerkonto for eksterne konsulenter

Eksterne konsulenter skal bruke Sykehuspartners HF utstyr og e-postadresse til Sykehuspartner-relatert formål. Dette innebærer at Sykehuspartners informasjon ikke skal sendes til egen virksomhets informasjonssystemer. Dersom det er formålstjenlig kan konsulenters utstyr og e-postadresse brukes, men dette skal begrunnes og avklares med oppdragsgiver på forhånd.

2.6 Regler for programvare

Sykehuspartner HF eier og er ansvarlig for all programvare som er installert på maskinen ved utlevering. Det enkelte helseforetak disponerer dette utstyret og programvaren.

Programvare skal normalt ikke installeres av bruker, med mindre dette er uttrykkelig godkjent. Bruker skal av sikkerhetsgrunner ikke endre oppsett på datamaskiner eller forsøke å omgå logiske eller tekniske sikringstiltak. Handlinger i strid med dette vil kunne påtales av arbeidsgiver. Sykehuspartner HF kan fjerne programvare hvis denne påvirker sikker og stabil drift av IKT.

2.7 Eierskap til data/informasjon

Virksomheten eier all virksomhetsrelatert informasjon. Dette gjelder alle personopplysninger, forskningsdata og administrative opplysninger. Bruk av slik informasjon utover virksomhetens behov er ikke tillatt. Bruk av andre offentlige registre som virksomheten har tilgang til, skal skje i tråd med de vilkår som er stilt for bruken.

2.8 Innsynsrett

Virksomheten har ved behov rett til innsyn i all informasjon lagret i informasjonssystemer. Innsynsretten har begrensninger og følger egne prosedyrer.

2.9 IKT-utstyr, inkludert medisinsk-teknisk utstyr

Det er ikke tillatt å benytte privat utstyr av noe slag i virksomhetens nett. Dette inkluderer, men er ikke begrenset til, nettbrett, mobiltelefon, kamera, minnekort og minnepinne.

Det er kun tillatt å benytte utstyr levert og installert av Sykehuspartner HF. Unntak fra dette skal være skriftlig avtalt med Sykehuspartner HF. Unntaket forutsetter sikkerhetsmessig risikovurdering og hvor det er konkludert med akseptabelt risikonivå av egen og Sykehuspartner HFs informasjonssikkerhetsleder.

Installasjon av alt utstyr og programvare skal gjøres av medarbeidere fra Sykehuspartner HF, eller av de som av Sykehuspartner HF er utpekt til å gjøre denne jobben. Unntak fra dette skal være skriftlig avtalt med Sykehuspartner HF, etter å ha vært gjenstand for sikkerhetsmessig risikovurdering som er akseptert i eget helseforetak og i overensstemmelse med Sykehuspartner HFs bruksvilkår.

Bruk av annen programvare eller maskinvare utenom det som virksomheten tilbyr som standard programvare, må godkjennes i henhold til foretakets prosedyrer for anskaffelser, IKT og informasjonssikkerhet.

Eksterne konsulenter og vikarer skal ikke koble til egne PC-er i virksomhetens nett, men få tildelt maskin av virksomheten. Særskilte behov for egne PC-er skal avklares med informasjonssikkerhetsleder. Det skal ikke tilkobles separate eksterne forbindelser til virksomhetens nett (for eksempel via ekstra nettverkskort, trådløst forbindelse/aksesspunkt, modem og lignende). Nettverkskort med direkte tilgang til eksterne nett/Internett skal aldri tilkobles.

IKT-utstyr skal ikke flyttes eller lånes til andre rom/lokaler uten avtale med Sykehuspartner HF. Dataskjermer skal plasseres slik at det ikke er innsyn for uvedkommende.

Medarbeidere som slutter eller går ut i permisjon, skal levere alt utlevert IKT-utstyr (mobil PC, mobiltelefon, nettbrett, sertifikat, brikke for fjerntilgang/passordkalkulator osv) og programvarelisenser til leder eller den leder beslutter, dersom ikke annet er avtalt.

Ta kontakt med Sykehuspartner HF dersom du har mistanke om feil eller problemer med tilgang til systemer, tjenester eller informasjon

Alt arbeid som skal utføres av eksternt personell på virksomhetens systemer og utstyr, skal bestilles gjennom Sykehuspartner HF.

2.10 Kassering/Håndtering av utstyr og lagringsmedier

Harddisker, minnepinner, minnekort, utstyr som inneholder harddisker og andre elektroniske lagringsmedier, skal leveres til Sykehuspartner HF for forsvarlig destruksjon. Lagringsmedia som CD, DVD, disketter osv. som inneholder personopplysninger (inkluderte kodede), eller media med andre opplysninger, skal leveres til Sykehuspartner HF for destruksjon. Pr. tid gjøres dette gjennom skjema i Min Sykehuspartner.

2.11 Lagring og behandling av personopplysninger

Det er som hovedregel kun tillatt å behandle sensitive personopplysninger i godkjente fagapplikasjoner i virksomhetens nettverk. Lagring og behandling av personopplysninger utenfor etablerte fagsystemer krever avklart lovlig grunnlag (samtykke, hjemmel i lov, godkjenning fra Personvernombudet, informasjonssikkerhetsleder eller REK, dispensasjon mm.). All behandling av personopplysninger skal være risikovurdert og godkjent før databehandling starter.

Bruk av ikke-fagsystemer som Word, Excel, SPSS mm. for behandling av personopplysninger skal kun benytte forhåndsgodkjente dedikerte filområder i henhold til virksomhetens prosedyrer.

Forskningsdata skal behandles i henhold til prosedyrer og rutiner for forskning. Kvalitetsregistre skal behandles i henhold til prosedyrer og rutiner for kvalitetsregistre.

Når lagringsmedia eller dokumenter med registre eller sensitive personopplysninger ikke er under direkte oppsyn, skal de oppbevares nedlåst eller sikres på annen måte slik at uvedkommende ikke får tilgang.

2.12 Kommunikasjon

Det skal utvises aktsomhet ved mottak av e-post. Vedlegg og linker kan inneholde virus. Ved tvil kan Sykehuspartner HF kontaktes eller e-postmeldingen slettes. Mottaker av e-post bør melde til avsender hvis mottaker åpenbart er feil adressat. Slike e-poster skal slettes.

2.13 Makulering/sletting av dokumenter

Dokumenter med personopplysninger som skal avhendes, skal makuleres ved bruk av makuleringsenhet, avlåste beholdere eller avlåste dedikerte rom for mellomlagring. Dersom ekstern leverandør benyttes for makulering, må det kontrolleres at dokumentene aldri er tilgjengelig for uvedkommende og at makulering skjer uten unødvendig opphold hos leverandør.

2.14 Opphør av arbeidsforhold

Medarbeidere som slutter, skal rydde i filområder og e-post og sikre at all relevant informasjon blir lagret på korrekt område. Arkivverdig informasjon skal lagres i virksomhetens sak/arkivsystem.

E-post og personlig filområde vil bli slettet omgående ved endt arbeidsforhold.

2.15 Sikkerhetskopiering

Det tas regelmessige sikkerhetskopier av all informasjon lagret i virksomhetens fagapplikasjoner og av virksomhetens filservere. For å sikre at det blir tatt sikkerhetskopier, skal all jobbrelatert informasjon lagres på eller eventuelt systematisk kopieres til virksomhetens fagapplikasjoner eller filservere.

Ved behov for rekonstruksjon av informasjon på sykehusnettet, kontakt Sykehuspartner HF.

Det blir ikke tatt sikkerhetskopier av informasjon lagret på lokale lagringsmedier som for eksempel minnepinner, eksterne harddisker eller lokal harddisk på ordinære PC-er i sykehusnettet. Informasjon på lokal harddisk på ordinære PC-er i sykehusnettet kan uten varsel bli slettet av Sykehuspartner HF.

2.16 Internett

Medarbeiderens oppslag på Internett kan spores tilbake til virksomheten og den PC/brukeridentitet som var i bruk da oppslaget ble gjort. Internett skal kun benyttes til lovlig aktivitet og i samsvar med vanlige etiske normer, slik at virksomhetsrelaterte oppgaver og funksjoner, samt opplysninger virksomheten behandler, ikke blir skadelidende.

Det er ikke tillatt å laste ned og installere programvare på virksomhetens IKT-utstyr uten godkjenning fra informasjonssikkerhetsleder. Bruk av fildelingstjenester er ikke tillatt.

2.17 Kartlegging og utnyttelse av systemsvakheter

Medarbeideren skal ikke på eget initiativ foreta kartlegging eller testing av mulige systemsvakheter, forsøke å trenge inn i interne eller eksterne systemer, forsøke å forbigå etablerte sikkerhetsmekanismer, tilegne seg utvidede tilgangsrettigheter på lokal maskin eller utnytte eventuelle sikkerhetssvakheter i informasjonssystemer eller infrastruktur.

Ved mistanke om svakheter, sårbarheter, feil eller mangler i informasjonssystemer, skal dette meldes Sykehuspartner HF.

2.18 Fysisk adgang

Alle medarbeidere, herunder innleide og andre som utfører arbeid på virksomhetens lokasjoner, skal bære gyldig ID-kort synlig og følge virksomhetens retningslinjer for fysisk adgang.

Den som mottar besøkende eller leverandører, er ansvarlig for at disse ikke oppholder seg i avlåste/avsperrede deler av virksomhetens lokaler uten følge av en medarbeider. Den enkelte medarbeider skal hindre at uvedkommende får adgang som kan gi tilgang til taushetsbelagte opplysninger eller annen beskyttelsesverdig informasjon og kritiske IKT-tjenester. Uvedkommen adgang skal varsles iht. foretakets rutiner.

2.19 Avvikshåndtering

Alle medarbeidere skal ved mistenkelige hendelser og observerte sikkerhetsbrudd, registrere avviket inn i virksomhetens avvikssystem i henhold til etablerte prosedyrer for avvikshåndtering, eller rapporteres til nærmeste leder, eller til informasjonssikkerhetsleder.

3. Signatur

Jeg har lest og forstått denne sikkerhetsinstruksen og forplikter meg til å overholde den.

Fornavn - Etternavn: _____

Brukernavn: _____

Stilling: _____

Virksomhet: _____

_____

Sted/dato **Signatur**

4. Vitnesignering for verifisering av identitet hos leverandør

Jeg (Vitne) signerer på at jeg har hatt et fysisk møte med personen som har signert på sikkerhetsinstruksen ovenfor, og at jeg ved dette møtet ble forevist et identitetsbevis som er godkjent for identifisering i Helse Sør-Øst.

Jeg signerer også på at

- Forevist identitetsbevis fremstår som ekte og gyldig
- Personen samsvarer med de fysiske kjennetegnene som er gjengitt på identitetsbeviset

Se sykehuspartner.no for kort veiledning i hvordan man vurderer om identitetsbevis er gyldig og om det er samsvar mellom en person og de fysiske kjennetegnene som er gjengitt på identitetsbeviset.

Marker hvilken bildelegitimasjon som er sjekket

Pass (norske og utenlandske)	
Norsk bankkort med legitimasjonsdel (bilde)	
Norsk førerkort utstedt f.o.m. 01.01.1998	
Europeisk identitetskort (Identity Card)[1]	

Navn: _____

Stilling: _____

Virksomhet: _____

_____ _____

Sted/dato Signatur

[1] Nasjonale ID-kort som er gyldig legitimasjon i EU og Schengen-landen