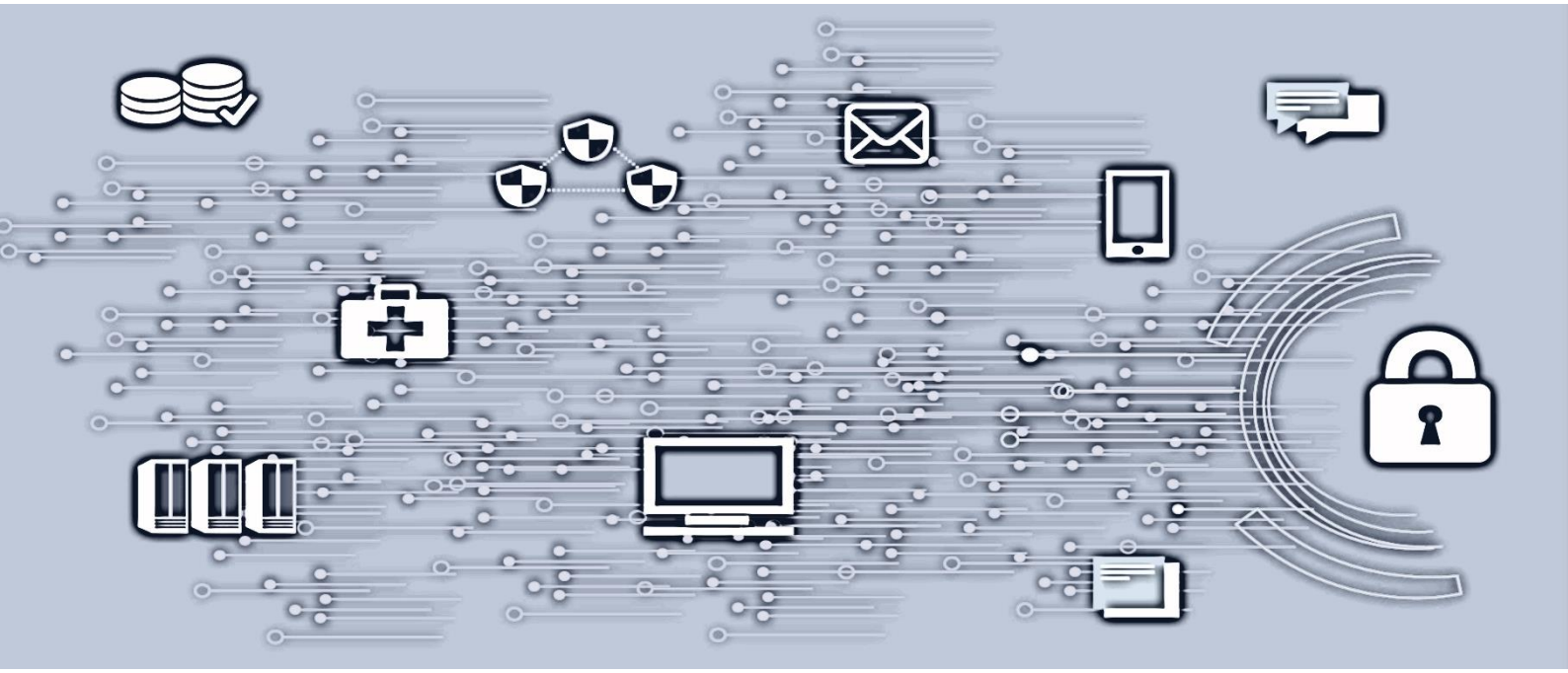
SYKEHUSPARTNER

# Sikkerhetssamtale 2022

**<medarbeiders navn, dato>**



# Innhold



| Versjon | Dato | Godkjent av |
|---|---|---|
| 2019 | N/A | Christian Jacobsen |
| 2020 | N/A | Christian Jacobsen |
| 2021 | N/A | Christian Jacobsen |
| 2022 | N/A | Christian Jacobsen |

# 1. Formål og omfang

Avdeling Sikkerhet er gitt ansvaret for sikkerhetsmessig internkontroll, herunder at ansatte mottar nødvendig sikkerhetsopplæring, at vedtatte sikkerhetsprinsipper etterleves, og at de besluttede sikkerhetskontroller fungerer i henhold til formålet.

Som en del av sikkerhetsmessig internkontroll gjennomføres **årlig en obligatorisk sikkerhetssamtale** mellom informasjonssikkerhetsleder og medarbeidere som jobber med informasjonssikkerhet i Sykehuspartner HF. Fra 2022 er det åpnet for deltagelse for øvrige ansatte i virksomheten. Samtalen er likevel primært ment for sikkerhetspersonell. Ved behov gjennomfører også informasjonssikkerhetsleder også en sikkerhetssamtale med innleid personell.

For de som har obligatorisk tilstedeværelse så signeres sikkerhetssamtaleskjema av begge parter etter gjennomført samtale. Informasjonssikkerhetsleder er gitt ansvaret for å arkivere det signerte dokumentet i den enkelte medarbeiders personalmappe. Dette gjøres ved årsslutt. Det er nærmeste leder som er ansvarlig for at sine ansatte deltar på den obligatoriske samtalen.

Sikkerhetssamtalen er ikke en erstatning for årlig utviklingsamtale med nærmeste leder.

**Agenda for 2022 er:**

1. Bakgrunn for sikkerhetssamtalen
2. Påminnelse om taushetsplikt
3. Dataminimering og andre prinsipper for databehandling
4. Plikt til å forhindre formålsutglidning
5. Akseptabel bruk av tilganger
6. Dokumentasjonsplikt
7. Plikt til å rapportere avvik, og hvordan disse meldes
8. Plikt til å gjennomføre sikkerhetsopplæring
9. Plikt til rapportering av risiko
10. Plikt til følge opp tiltak
11. Delingskultur internt og eksternt
12. Forventninger til adferd internt og eksternt
13. Forholdet til sikkerhetsloven

Innholdet i sikkerhetssamtalen kan endre seg fra år til år. Om den enkelte medarbeider ser behov for supplering til sikkerhetssamtalen, kan dette sendes til informasjonssikkerhetsleder

# 2. Bakgrunn for sikkerhetssamtalen

Sykehuspartner HF er landets største databehandler av helseopplysninger. Det har over tid blitt bygget opp et vesentlig fagmiljø for å ivareta disse personopplysningenes konfidensialitet, integritet og tilgjengelighet særlig med det formål å beskytte mot den fare som trusselaktører utgjør.

Sykehuspartners visjon er å være en partner for helsetjenester i utvikling, og målbildet vårt er at vi er den foretrukne teknologi- og tjenestetilbyderen som gjør informasjon tilgjengelig for dem som trenger det. Sikkerhetsmiljøene skal bistå til at Sykehuspartner HFs målbilde realiseres. Dette gjør vi ved å kombinere en forholdsmessig risiko mot ønsket gevinst.

For å oppnå et tilfredsstillende sikkerhetsnivå som reduserer risiko for at uønskede hendelser inntreffer og dermed også forhindrer oss i å nå våre mål, har virksomheten valgt å ta i bruk verktøy som gir mange i sikkerhetsmiljøet en stor grad av tilganger, både på endepunkter og i nettverket, eller gjennom saksbehandling og avviksmeldinger. Disse tilgangene er gitt under klare forutsetninger, og misbruk tolereres ikke.

Fagmiljøene har ulik kompetanse, faglig bakgrunn og utdanning. Det er derfor ønskelig for Sykehuspartner å sikre at personell som arbeider med informasjonssikkerhet er kjent med regelverket virksomheten er underlagt.

## 3. Påminnelse om taushetsplikten

Alle som utfører arbeid på vegne av Sykehuspartner HF er underlagt generell, forvaltningsmessig taushetsplikt, dette følger av forvaltningslovens bestemmelser. Dette betyr at den enkelte har en plikt til å sørge for at taushetsbelagte opplysninger ikke gjøres kjent for allmennheten. Medarbeidere som kommer i befatning med helseopplysninger vil også kunne bli underlagt de samme taushetsregler som gjelder for helsepersonell, jf. helsepersonelloven § 25, 4. ledd (samarbeidende personell). Dette kalles ofte profesjonsbasert taushetsplikt.

Med taushetsbelagt materiale forstås både helse- og personopplysninger og andre opplysninger som kan anses som taushetsbelagte (eksempelvis forretningshemmeligheter). Opplysningene kan være interne, eies av helseforetakene eller andre.

Taushetsplikten gjelder ovenfor venner, familie, kolleger og andre. Taushetsplikten betyr også en plikt til å oppbevare taushetsbelagt materiell på godkjente områder, hvor både prinsippet om tilgangsstyring og sporbarhet ivaretas. Dette omfatter for eksempel datapakkefiler, loggfiler, rapporter, avvik eller andre type opplysninger som er hentet ut fra et informasjonssystem. Slikt materiale kan kun lagres på godkjente områder.

Brudd på taushetsplikt skal ikke forekomme. Det vil være særdeles skjerpende om ansatte i sikkerhetsmiljøet, som både har svært vide tilganger og som skal utøve sitt yrke med en høy grad av integritet, bryter taushetsplikten. Eventuelle brudd på taushetsplikten kan medføre ulike reaksjoner basert på alvorligheten av omfanget, eksempelvis tap av tilganger, oppsigelse, avskjed og straffansvar. Sykehuspartner er underlagt offentlighetsloven og det er ønskelig med en åpenhetskultur. Alle våre medarbeidere, også ansatte i som jobber med informasjonssikkerhet, har ytringsfrihet. Grensen mellom taushetsplikt, offentlighetsloven og ytringsfrihet kan i noen tilfeller være vanskelig. Er du usikker kan du ta kontakt med informasjonssikkerhetsleder for veiledning.

## 4. Dataminimering og andre prinsipper for databehandling

Artikkel 5 i den felleseuropeiske personvernforordningen («GDPR») definerer 7 grunnpilarer for databehandling av personopplysninger:

- Ansvarlighet,
- Lovlighet, rettferdighet, gjennomsiktighet,
- Riktighet,
- Dataminiminering
- Formålsbegrensning
- Lagringsbegrensning
- Integritet og fortrolighet

Vi skal se nærmere på noen av disse.

Lagringsbegrensningen pålegger dataansvarlige og databehandlere (som Sykehuspartner HF) en begrensning på å ikke oppbevare data lenger enn nødvendig (*kept in a form which permits identification of data subjects for no longer than is necessary*). Dataminimering handler om å begrense innsamlingen til det som er nødvendig for å kunne gjennomføre oppdraget (*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*).

Disse grunnpilarene er gjeldende for hele Sykehuspartner HF, også sikkerhetsmiljøet. Det betyr at jeg som informasjonssikkerhetsleder må være sikker på at medarbeidere i informasjonssikkerhetsmiljøet i Sykehuspartner HF, uansett om det er avvik, incidenter, revisjoner e.l. forstår disse konseptene, at dere sørger for at arbeid utføres i tråd med disse prinsippene. Eventuelle mislighold eller avvik skal rapporteres på en forsvarlig måte.

## 5. Plikt til å forhindre formålsutglidning

Et annet grunnkonsept i Artikkel 5 i GDPR er Formålsbegrensning, hvilket betyr at data kan kun brukes til det formålet det er samlet inn (*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*). All databehandling av personopplysninger skal ha et gyldig formål.

En sentral begrensning ved all databehandling er at personopplysninger som er samlet inn til et formål ikke kan brukes til et annet formål som er uforenelig med det opprinnelige formålet. Skal innsamlede personopplysninger brukes til et annet formål, så skal bruken skal være hjemlet i lov eller være basert på samtykke, jf. artikkel 6, 4. ledd. Hovedregelen er altså at personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål.

For sikkerhetsmiljøet er begrepene formålsbegrensning og formålsutglidning svært viktige. Når vi behandler personopplysninger, må vi også være sikre på at vi har lov til å behandle dataene (lovlighetsprinsippet). Som hovedregel kan vi ikke be om samtykke fra de registrerte for de dataene vi innsamler (enten det er pasienter, pårørende, ansatte i helseforetaket, forskere, leverandører eller andre), og vi må derfor sikre at vi har lovlig hjemmel for databehandlingen. Som nevnt over må denne være spesifikk, uttrykkelig, angitt og legitim. F.eks. PCAP-data innsamlet for analyseformål kan ikke benyttes til f.eks. å sjekke om den ansatte kom på jobb tidsnok, fordi formålet med analyseplattformen ikke er å være et kontrolltiltak i HR-aksen.

## 6. Akseptabel bruk av tilganger

Tilgangsnivået i sikkerhetsmiljøet er svært ulikt. Det operative miljøet har som hovedregel videre tilganger enn det strategiske, men dette er også en regel med unntak. Like fullt er hovedprinsippet for tilgang det samme: tilgang skal følge tjenstlig formål og skal ikke være videre enn det som er absolutt nødvendig for å kunne utføre sitt yrke.

Det er en klar og tydelig forventning fra meg som informasjonssikkerhetsleder at alle ansatte i alle aspekter av informasjonssikkerhet og personvern i Sykehuspartner forstår og respekterer dette. Det vil være et alvorlig tillitsbrudd om medarbeidere i informasjonssikkerhetsmiljøet gir seg selv, eller sine kolleger, rettigheter uten godkjenning eller utenfor saksbehandlingssystemet. Slike aktiviteter

kan medføre risiko for inndragelse av rettigheter eller konsekvenser for arbeidsforholdet. Tilganger skal også opphøre når det tjenstlige behovet opphører.

For Sikkerhetsplattformen og Sikker Sone så følger det egne prosedyrer for tilgangsstyring, hvor Sykehuspartner HFs request-prosess ikke benyttes. Forventningen for Sikkerhetsplattformen er helt lik som den er for produksjonsplattformen SIKT: tilgangene skal være sporbare, de skal være basert på tjenstlig behov, og prinsippene om sporbarhet og uavviselighet (når tilganger ble gitt og begrunnelsen for at de ble gitt) skal ivaretas. Kravet er altså ikke på noen måte annerledes for Sikkerhetsplattformen enn for SIKT.

Det er også en forventning om at medarbeidere som benytter lovlige tilganger til informasjonssystemer, ikke benytter disse tilgangene på en måte som utfordrer hverken det juridiske eller etiske regelverket. Snoking eller annen form for å oppsøke personopplysninger uten godkjent formål er strengt forbudt, og vil være et alvorlig tillitsbrudd og kan medføre oppsigelse, avskjed og straffansvar. Dette inkluderer ikke utelukkende kliniske systemer, men også f.eks. maillogger, surfelogger eller andre IKT-logger som gjelder den enkelte ansatte. Dette gjelder også for bruk av sikkerhetsverktøy som Carbon Black. Det er min forventning at den enkelte medarbeider klarer å gå disse grenseoppgangene selv, og når man er i tvil så spør man informasjonssikkerhetsleder eller nærmeste leder om bistand.

## 7. Dokumentasjonsplikt

Den enkelte medarbeider må sørge for at man utfører en forsvarlig grad av dokumentasjon og arkivering. Hendelser, avvik, saksforberedelser mv. skal dokumenteres på en tilfredsstillende måte. De ulike fagmiljøene er selv ansvarlige for at nødvendig dokumentasjon utarbeides og vedlikeholdes.

Arkivverdig dokumentasjon skal arkiveres i Public 360. Nærmeste leder kan bistå med dette. System- og driftsdokumentasjon skal lagres på egnet område. Saks- og hendelsesinformasjon skal lagres i de systemene som er besluttet for dette formålet.

Tjenestedokumentasjon skal holdes oppdatert. Dette gjelder også for sikkerhetsporteføljen. Systemdokumentasjon og systemkonfigurasjon skal være sammenfallende. Endringer skal kunne spores og være godkjent i tråd med de til enhver tid gjeldende prosedyrer.

## 8. Plikt til å rapportere avvik, og hvordan disse meldes

Sykehuspartner HF skal være en lærende virksomhet, og behandlingen av avvik er en hovedkilde for at vi skal kunne gjennomføre kontinuerlig forbedring. For at dette forbedringssystemet skal fungere, må avvik rapporteres og håndteres. Sikkerhetsmiljøet er sannsynligvis et av fagmiljøene i hele Helse Sør-Øst som kommer i kontakt med flest avvik – og kanskje også noen av de mest kompliserte avvikene.

Som informasjonssikkerhetsleder er det mitt mål at alle mine kolleger skal føle at rapportering av avvik er et gode for virksomheten; det er en kilde til forbedring og lærdom. Det er min forventning at alle skal føle seg trygge på å melde avvik, og at innrapportering av avvik skal skje uten frykt for represalier.

Det er min forventning at ansatte som jobber med informasjonssikkerhet går foran som gode eksempler når det gjelder rapportering av avvik. Dette gjelder også historiske avvik som dere kjenner

til. Det er ikke tilfredsstillende om avvik som «alle» kjenner til ikke blir dokumentert «fordi det alltid har vært slikt».

Avvik skal også rapporteres selv om en hendelse har blitt løst eller tiltak har blitt satt i verk. Avviket kan da meldes som avsluttet, men vil likevel inngå i rapporteringen vår.

## 9. Plikt til å gjennomføre sikkerhetsopplæring

Som informasjonssikkerhetsleder forventer jeg at ansatte i sikkerhetsmiljøene er godt kjent med sikkerhetsbestemmelsene i virksomheten, og at vi fremstår som foregangsmodeller i vår etterlevelse. Våre holdninger og adferd relatert til informasjonssikkerhet vil bli lagt merke til av mange rundt oss.

Alle ansatte i Sykehuspartner HF skal gjennomføre obligatoriske kurs innen informasjonssikkerhet og personvern, og det forventes at alle ansatte gjør seg kjent med sikkerhetsinstruksen. Dette gjelder naturligvis også ansatte i sikkerhetsmiljøet.

## 10. Plikt til rapportering av risiko

God risikostyring gir grunnlag for god virksomhetsstyring, og legger til rette for at gode beslutninger tas. Informasjonssikkerhet skal være en del av grunnleggende virksomhetsstyring. Risiko innenfor informasjonssikkerhetsområdet kan potensielt påvirke virksomhetens totale måloppnåelse, og alvorlige hendelser innen det digitale rom kan gi reelle konsekvenser for menneskers liv og helse.

Sykehuspartner har etablert en prosess for risikostyring. Som informasjonssikkerhetsleder forventer jeg at alle i sikkerhetsmiljøet aktivt bistår i risikoarbeidet i egen organisasjonsenhet, ved at risiko dokumenteres og løftes.

Sikkerhetsmiljøene skal bestrebe en faglig forsvarlig, edruelig og fakta-orientert risikorapportering. Vurdering av konsekvens og sannsynlighet skal være faktabelagt, og så langt som mulig skal empiri legges til grunn, særlig ved fastsettelse av sannsynlighet, i tillegg til vurdering av nåværende tiltaksstatus og vurdering av fremtidig trend. For fastsettelse av sannsynlighet og konsekvens skal regional risikoskala for informasjonssikkerhet benyttes. Veileder for fastsettelse av sannsynlighet og konsekvens kan med fordel brukes som hjelpemiddel.

Det skal utarbeides tiltaksoversikt for å redusere risiko. Tiltakene skal være forholdsmessige ut fra et kost/nytte-perspektiv, med andre ord: negativ konsekvens ved innføringen av tiltaket skal være mindre enn negativ risiko om den uønskede hendelsen inntreffer.

## 11. Plikt til å følge opp tiltak

Gjennom risikovurderingsprosessen tildeles tiltak til en tiltakseier. Tiltakseieren er altså ansvarlig for at tiltaket faktisk gjennomføres. Tiltakseier skal alltid være kjent med og akseptere ansvaret for tiltaksgjennomføringen før tiltaket settes til vedkommende.

Tiltakseier plikter å følge opp sine tiltak slikt tiltaket er overlevert. Tiltaksoppfølgingen er et ledelsesansvar. Det forventes at risikoeier informeres om et tiltak ikke lar seg implementere innen tid eller innen avtalt omfang.

## 12. Delingskultur internt og eksternt

Sykehuspartner HF skal tilstrebe seg en åpen og ærlig kommunikasjon om informasjonssikkerhet, både med interne og eksterne parter. Sykehuspartner HF skal ha en særlig god kommunikasjon med våre kunder, eiere, offentlige tilsynsmyndigheter og øvrige sikkerhetspartnere.

Vi skal være kjent med, følge og benytte Trafikklysprotokollen (TLP) i tråd med beste praksis, og vi skal skape tillit hos våre samarbeidspartnere. Vi skal aktivt dele informasjon, erfaringer og anbefalinger fra egne organisasjon som gjør aktører rundt oss gode, og når aktører rundt oss velger å dele med oss, skal vi behandle den informasjonen i tråd med avsenders TLP-klassifisering.

## 13. Forventninger til adferd internt og eksternt

Vi skal tilstrebe oss et omdømme som pålitelige, kompetente, imøtekommende og effektive. Vi har som en del av våre arbeidsoppgaver et særlig ansvar for at resten av organisasjonen føler tillit til oss, og vi skal være kontinuerlig oppmerksom på at vår adferd ikke undergraver denne tilliten. Vi skal behandle våre kolleger på en profesjonell, vennlig og forutsigbar måte.

Eksternt skal vi representere Sykehuspartner HF på en god måte. Som informasjonssikkerhetsleder ser jeg at vårt omdømme er bundet opp mot den adferd hver enkelt av oss utøver i det offentlige rom. Vis måtehold med alkohol når du representerer sikkerhetsmiljøet, utøv et fornuftig skjønn ved bruk av sosiale medier der hvor ditt navn kan kobles opp til din rolle i Sykehuspartner HF og vær bevisst hvordan du opptrer i sammenhenger hvor andre kan oppfatte at du opptrer i en profesjonell sammenheng.

Vi skal også være en attraktiv arbeidsgiver, også for ny og ung kompetanse. Hvordan vi tar imot nye kolleger er derfor relevant for hvordan vi oppfattes. Det er mitt mål, både som avdelingsleder for avdeling Sikkerhet og som informasjonssikkerhetsleder, at vi skal ha en bredt sammensatt gruppe medarbeidere, både mht. kjønn, alder, bakgrunn, livssyn, og så videre. Vi skal dermed ha takhøyde og respekt for hverandre. Vi skal bidra til å ha en kultur hvor vi snakker hverandre opp på tvers av fagmiljø og organisasjonsenheter og jeg forventer alle bruker tid på å reflektere over hva Sykehuspartner HFs verdier (fremoverlent, ansvarlig, medspiller) betyr, og hvordan du som en del av en større organisasjon kan bidra til å skape et godt sikkerhetsmiljø.

Jeg forventer at informasjonssikkerhetsmiljøet skal være et trygt sted å jobbe. Dette gjelder også uønsket seksuell oppmerksomhet mot kolleger. Vi kan aldri bli et inkluderende miljø om ikke alle føler seg trygge på jobb.

## 14. Forholdet til sikkerhetsloven

Sykehuspartner HF er underlagt sikkerhetsloven, og har etablert en egen sikkerhetsorganisasjon til dette formålet. Som del av offentlig forvaltning, og som regional databehandler for Helse Sør-Øst, er det tenkelig at du som medarbeider vil komme i kontakt med gradert materiell. Når dette er nødvendig, er det sikkerhetsleder som gjennomfører klareringssamtale før det blir gitt tilgang til gradert materiell. De som er autorisert etter sikkerhetsloven følges opp med egne autorisasjonssamtaler.

Helsesektoren skal understøtte **Grunnleggende Nasjonale Funksjoner**, herunder helseberedskap og evnen til å yte nødvendig, akutt og elektiv, livsbevarende helsehjelp.

Det er departementet som utpeker skjermingsverdige objekter, informasjonssystemer eller informasjon, basert på verdi- og skadevurderinger som Sykehuspartner HF utfører. Listen over graderte objekter, informasjonssystemer eller informasjon gjøres kjent for den enkelte på et «need to know»-prinsipp.

Personell som blir autorisert føres inn i virksomhetens autorisasjonsliste. Her er man registrert inntil autorisasjonen opphører. Man er kun autorisert for den konkrete informasjonen eller det konkrete objekter som autorisasjonssamtalen dekker. Personell som skal sikkerhetsklareres skal fylle ut personopplysningsblanketten. Klareringsmyndigheten vår er Sivil Klareringsmyndighet. Etter klarering vil klareringsbevis oppbevares av Sykehuspartner HF v/ avd. Sikkerhet frem til klarering utgår, eller arbeidstager avslutter arbeidsforholdet. Ved behov for kopi av klareringsbevis må medarbeider henvende seg til avd. Sikkerhet i forkant.

Etter sikkerhetsloven er begrepet skikkethet benyttet for å definere hvorvidt en person er egnet for å håndtere sikkerhetsgradert informasjon, ha adgang til sikkerhetsgraderte objekter, eller ha tilgang til sikkerhetsgraderte informasjonssystemer, infrastrukturer eller informasjon.

Personell som blir autorisert eller sikkerhetsklarert vil ha egne samtaler med sikkerhetsansvarlig, som vil være langt mer inngående i subjektets plikter og rettigheter. Skulle Sykehuspartner HF på et tidspunkt finne grunn til å vurdere at en medarbeider som er klarert potensielt ikke fortsatt kan anses å være sikkerhetsmessig skikket, så påfaller det Sykehuspartner HF en plikt å varsle Sivil Klareringsmyndighet om dette. For sikkerhetsklarert personell så minner jeg om varslingsplikten om det oppstår forhold som kan påvirke skikkethet.

Sykehuspartner HF har også mulighet for digital, gradert kommunikasjon gjennom Nasjonalt Begrenset Nett. Ved behov for å bruke dette verktøyet, kan avd. Sikkerhet kontaktes.

Gradert informasjon skal føres i gradert postjournal. Utlånt gradert informasjon skal leveres tilbake. Skulle du motta gradert materiell du ikke er autorisert for, kontakt informasjonssikkerhetsleder omgående.

Det er pr. dag ikke et generelt krav om sikkerhetsklarering for å arbeide i informasjonssikkerhetsmiljøet i Sykehuspartner HF, men et slikt krav kan bli stilt senere.

## 15. Signatur

Sikkerhetssamtalen mellom Informasjonssikkerhetsleder og <medarbeider> er gjennomført <dato>.

_____ _____

Medarbeider Informasjonssikkerhetsleder