

Sikkerhetsinstruks for ansatte og innleid personell i Norsk helsenett

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren. Norsk helsenett knytter helsetjenesten sammen og gjør helsedata og IKT-tjenester tilgjengelig for helseforvaltningen, helsepersonell, pasienter og befolkningen ellers – trygt og enkelt. Norsk helsenett består av to tjenesteområder:

- Felles tjenestesenter, som leverer tjenester innen IKT, arkiv og anskaffelser til den sentrale helseforvaltningen
- Nasjonal tjenesteleverandør som leverer drift, utvikling og forvaltning av nasjonale e-helseløsninger til hele helsetjenesten, og som bidrar til effektiv digital informasjonsflyt i sektoren, og dermed effektiv pasientbehandling

Gjennom disse tjenesteleveransene forvalter Norsk helsenett helseinformasjon og andre personopplysninger om hele Norges befolkning, i tillegg til virksomhetsinformasjonen til våre kunder og vår egen virksomhet. Tjenesteleveransene fra Norsk helsenett inngår i lengre digitale verdikjeder i helsetjenesten og understøtter nasjonale beredskapsfunksjoner. Nedetid eller datainnbrudd i de mest sentrale tjenestene kan få katastrofale følger for norsk helsetjeneste. For eksempel i form av betydelig redusert kapasitet til pasientbehandling og fare for liv og helse, svekket nasjonal helse- og atomberedskap, eller alvorlige brudd på menneskerettslige krav til personvern. Personverns- og sikkerhetsbrudd kan dessuten medføre betydelig tappt tillit i sektoren og i befolkningen, noe som igjen påvirker helsetjenestens evne til å utvikle nye digitale løsninger.

Denne sikkerhetsinstruksen stiller krav og forventninger til hver enkelt ansatt i Norsk helsenett, inkludert innleid personell, knyttet til forsvarlig bruk av våre IKT-systemer og forsvarlig håndtering av informasjon som krever skjerming. Når du følger disse kravene, bidrar du til at Norsk helsenett forblir en trygg tjenesteleverandør.

Sett deg inn i hva som kreves av deg i din rolle

- Du har et selvstendig ansvar for å sette deg inn i, og etterleve, de sikkerhetskrav og regler som gjelder for den jobben og de oppgavene du gjør i Norsk helsenett. Vårt styringssystem for sikkerhet og personvern gir de overordnede rammene for sikkerhets- og personvernsarbeidet. Styringssystemet finner du på følgende Sharepoint side: Sikkerhet, personvern og beredskap i NHN (<https://nhnkontor.sharepoint.com/sites/Sikkerhet>). Viktige endringer i styringssystemets retningslinjer og andre styrende dokumenter vil bli kommunisert via Intravenøs og som nyheter på Sharepoint siden.
- Du er underlagt taushetsplikt i henhold til den taushetsplikterklæringen du skriver under på ved oppstart. Denne finner du i personalhåndboken ([Norsk Helsenett SF :: Personalhåndbok :: Taushetsplikt \(compendia.no\)](#))
- Vær varsom med tanke på hvem du deler virksomhetskritisk og sensitiv informasjon med. Tenk over hva du sier, og særlig når du snakker om jobb utenfor kontoret når utenforstående kan høre deg.

- Norsk helsenett skal sørge for at du får den sikkerhetsopplæringen du trenger. I tilfeller der du er usikker på hvilke krav som gjelder, eller hvordan de skal etterleves skal du alltid søke råd hos din leder, kolleger eller hos en sikkerhetsleder.

Sikker håndtering av passord og smartkort/tokens

- Passordene (og smartkort/tokens) som du bruker mot Norsk helsenett sine IKT-systemer er personlige. Du skal aldri oppgi, eller utlevere dem til andre.
- Du skal ikke gjenbruke passord på tvers av IKT-systemer, hverken internt i Norsk helsenett eller mot eksterne tjenester.
- Dersom du har mistanke om at passordet ditt har blitt kjent av uvedkommende, skal du snarest mulig bytte passordet ditt og rapportere hendelsen til nærmeste leder.

Sikker bruk av e-post

- Dersom e-post skal benyttes til å overføre informasjon som krever skjerming bør du sørge for tilstrekkelig kryptering av innholdet – for eksempel gjennom å sende en kryptert og passordbeskyttet fil.
- Som hovedregel skal du ikke sende **helseopplysninger** eller virksomhetskritisk informasjon på e-post.
- Vedlegg og lenker skal ikke åpnes dersom du ikke stoler på innholdet. Husk at e-poster konstruert for phishing kan se ut til å komme fra en kollega.
- Du skal ikke sette opp automatisk videresending av e-post fra din e-postkonto fra Norsk helsenett til privat e-postkonto eller e-postkonto hos annen arbeidsgiver.
- Du har selv ansvar for å opprette egen mappe som tydelig er merket 'PRIVAT', for lagring av privat e-post. Som hovedregel skal du kun bruke din e-postadresse og konto fra Norsk helsenett til arbeidsrelaterte formål.

Akseptabel bruk av tjenester på Internett

- Internett skal som hovedregel brukes til arbeidsrelaterte formål, slik som i forbindelse med e-post og innhenting av informasjon. Det er tillatt med noe privat bruk. Eksempler på akseptabel og uakseptabel bruk:

Akseptabel bruk

- Nettbasert privat e-post, nettaviser, nettbank, hjemmesider og informasjonssider
- Alle arbeidsrelaterte formål

Uakseptabel bruk

- Tjenester som unødvendig belaster nettverket og hvor det ikke er tjenstlig behov
- Oppslag på nettsteder som kan skade Norsk helsenetts omdømme eller sikkerhet. (Eksempler: pornografi, gambling, og nettsteder som det er grunn til å anta at innebærer risiko for spredning av skadegjennomvare.
- Tjenester eller aktiviteter som er i brudd på norsk lov og åndsverkregler

- Brudd på Norsk helsenetts etiske retningslinjer, som er beskrevet i personalhåndboken.

Sikkerhet på kontoret, inkludert hjemmekontor

- Dokumenter som inneholder skjermet eller sterk skjermet informasjon skal ikke ligge åpent tilgjengelig for uvedkommende.
- Når du forlater PC/Mac i løpet av arbeidsdagen skal du låse skjermen.
- PC/Mac du har fått utlevert fra Norsk helsenett skal kun benyttes av deg selv, eller andre ansatte i Norsk helsenett (med egen brukerkonto). Det er for eksempel ikke tillatt å låne ut PC/Mac til familiemedlemmer.

Sikkerhet på reise

NHN PC/Mac skal ikke medbringes på private reiser (ferie) til utlandet. Dersom du mot formodning har et kritisk behov for å jobbe i utlandet mens du er på privat reise skal retningslinje om "Jobb utenfor Norge i forbindelse med private reiser" følges.

Ved reise til PST definerte høyrisikoland (Russland, Kina, Nord-Korea, Iran og Pakistan) skal både NHN PC/Mac og mobiltelefon koblet til NHN sin infrastruktur ligge igjen hjemme. Flere detaljer finner du i styringssystemet og standard "S09 Standard for bruk av utstyr på reise til risikoland".

Ved forretningsreiser og ved eventuelle private reiser, må du ivareta følgende:

- Sikre at utstyret er oppdatert med siste versjoner av operativsystem/programvare før du reiser.
- Sørg for at PC/Mac er innelåst når utstyret ikke brukes. Lås døren til hotellrommet og gjerne benytt en safe på hotellet hvis tilgjengelig.
- Logg helt ut og slå av PC/Mac når den ikke brukes. Da er den sikrere i tilfelle tyveri.
- Meld fra så raskt som mulig hvis mobiltelefon eller PC/Mac kommer på avveie. Ta kontakt med Operasjonssenteret i Trondheim, +47 73 56 59 99.
- Vær bevisst på hvor/hvordan du fysisk sitter og jobber, slik at du hindrer innsyn. Bruk gjerne ett skjerfilter.
- Unngå generelt bruk av Wi-Fi som ikke krever et passord for tilkobling, og benytt kun kjente Wi-Fi-nettverk. Unngå bruk av offentlige, gratis Wi-Fi f.eks. på hoteller, caféer, på flyplasser, eller på konferanser. Bruk heller mobilt bredbånd eller din mobiltelefon til internett-delning (4/5G mobildata) innenfor EU/EØS der roaming ikke medfører ekstra kostander.

Utskrift, kopiering og makulering

- Norsk helsenett har etablert løsning for sikker utskrift. Du må identifisere deg med adgangskortet for å skrive ut dokumenter.
- Dokumenter som inneholder informasjon som krever skjerming må ikke bli liggende på kopimaskin/skriver.
- Dokumenter eller notater som inneholder skjermingsverdig informasjon skal du ikke kaste i vanlig søppelkasse. Bruk kontainer for sikkerhetsmakulering.

Bruk av Norsk helsenett sine IKT-systemer

- Våre informasjonssystemer er beregnet for jobbrelaterte formål. Du skal begrense privat bruk slik at bruken ikke påvirker jobbrelaterte oppgaver, eller forstyrrer tekniske løsninger og sikkerheten i IKT-infrastrukturen.
- Vi skal bare bruke NHNs systemer (egenutviklet eller anskaffet iht. NHNs anskaffelsesprosess) når vi jobber. Det betyr at virksomhetsrelatert informasjon (inkludert personopplysninger) ikke skal lagres eller på annen måte behandles på privat utstyr eller i kommersielle lagringstjenester anskaffet i privat regi. Denne typen informasjon skal heller ikke brukes i kommersielt tilgjengelige tjenester [på internett] som f.eks. ChatGPT
- Du skal kun installere programvare som er distribuert gjennom NHNs firmaportal på din jobb PC. Ved behov for ytterligere programvare skal dette bestilles gjennom brukerstøtte.
- Du skal ikke forsøke å omgå sikkerhetsmekanismer i Norsk helsenetts infrastruktur.
- Du skal ikke ha angrepsverktøy eller skadelig programvare på din PC/Mac
- Du skal ikke koble privat utstyr inn i Norsk helsenett sine interne nettverk, med unntak av godkjente BYOD (bring your own device) klienter i utviklingsnett (se også S10 Standard for klientsikkerhet)
- Når IKT-utstyr skal kasseres, eller du ikke lenger skal bruke det til arbeidsformål, er du ansvarlig for at utstyret leveres tilbake til Norsk helsenett for sikker destruksjon.

Fysisk adgang til våre lokaler

Adgangskort

- Dersom du mister adgangskort og ev. nøkler, meld umiddelbart fra til lokasjonsansvarlig eller sikkerhetsleder.
- Medarbeider som slutter skal levere adgangskort og evt nøkler tilbake til nærmeste leder senest ved siste arbeidsdag.
- Du skal bære adgangskort synlig, og oppfordre andre til å gjøre det samme.
- Dersom du ser personer som forsøker å ta seg inn i lokalene uten synlig adgangskort skal du ikke slippe dem inn i lokalene, men eventuelt hjelpe dem med å kontakte den personen de skal besøke.

Besøkende

- Dersom du tar imot besøkende i NHNs lokaler, har du ansvaret for vedkommende under hele besøket. Besøkende skal hentes og følges ut av NHN sine kontorlokaler

Kontakt med media

- Det er kun administrerende direktør, direktør for organisasjon og kommunikasjon, eller den han/hun gir ansvaret til (eksempelvis pressevakt) som har myndighet til å uttale seg til presse eller andre media i forbindelse med saker som gjelder Norsk helsenett.

Rapportering og avvik

- Oppdager du avvik tilknyttet sikkerhet og personvern skal disse uten opphold meldes inn i henhold til [rutiner for avvikshåndtering](#).

Spesielle vilkår som gjelder for arbeidsgivers styringsrett

Innsyn i e-post og filer

- Norsk helsenett har som hovedregel ikke anledning til innsyn i privat e-post eller filer. Unntak gjelder når det er nødvendig for å ivareta driften av virksomheten eller dersom det er mistanke om grove brudd på arbeidstakers plikter. Som hovedregel skal du varsles og kunne være til stede ved innsynet. Norsk helsenett er underlagt reglene i forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk materiale i slike tilfeller. Datatilsynets veileder om arbeidsgivers innsyn og NHNs rutine i styringssystemet ([Rutine for arbeidsgivers innsyn i e-post og filområder \(sharepoint.com\)](#)) gir mer veiledning.

Logging

- Aktivitet i og bruk av våre IKT-systemer og utstyr blir logget for å ivareta nødvendig sikkerhet i våre systemer. Loggene blir brukt for å sikre god og stabil drift og for å kunne oppdage og håndtere sikkerhetstruende hendelser (cyberangrep, datavirus, m.m.). Norsk helsenett benytter også verktøy som sikrer sporbarhet i bruk av privilegerte og ikke-privilegerte kontoer, for å kunne dokumentere hva som faktisk er gjort og av hvem. Dette er også beskrevet i personvernerklæringen som er en del av [personalhåndboken](#).

Konsekvenser ved brudd på sikkerhetsinstruksen

Konsekvenser for medarbeidere som har brutt sikkerhetsreglene vil bli vurdert i hvert enkelt tilfelle, og kan ved alvorlige brudd føre til oppsigelse/avskjed, ref. personalhåndbokens avsnitt om avskjedigelse.

Sikkerhetsinstruksen er lest og akseptert:

Sted og dato: _____

Navn (blokkbokstaver): _____

Signatur: _____