SIKKERHETSINSTRUKS FOR BRUKERE I NORSK HELSENETT

INNLEDNING

Denne instruksen beskriver retningslinjer for bruk av IT ved Norsk Helsenett SF (NHN). Instruksen gjelder for alle ansatte, vikarer og innleide (heretter kalt brukere), og skal være lest og signert, og så avleveres til arkivering.

BRUK AV NHN SITT INFORMASJONSSYSTEM

- Dokumenter som inneholder beskyttelsesverdige opplysninger som kan skade enkeltindivider, kunder eller NHN, hvis de blir kjent av uvedkommende, skal graderes, merkes og håndteres i henhold til rutine for informasjonshåndtering.

- NHNs informasjonssystemer er beregnet for jobbrelaterte formål. Privat bruk, f.eks. e-post og private filer tillates i begrenset omfang, så lenge det ikke påvirker jobbrelaterte oppgaver.

- NHN har i utgangspunktet ikke anledning til innsyn i privat e-post eller filer. Unntak gjelder hvis du er ikke-planlagt utilgjengelig i lengre tid, og virksomheten har behov for virksomhetsrelatert informasjon. NHN følger datatilsynets retningslinjer ved innsyn.

- All jobbrelatert informasjon skal lagres på filservere eller dedikerte informasjonssystemer, slik som f.eks. Confluence. Hjemmekatalogen skal primært brukes for informasjon som den enkelte ønsker å ta vare på, og som kan benyttes på tvers av prosjekter eller funksjoner som vedkommende utfører. Det skal ikke lagres private data på disse områdene.

- Utskrifter skal fjernes fra skriveren så snart utskriftsjobben er ferdig.

- Alle lagringsmedia skal merkes og krypteres hvis de benyttes til helse- og personopplysninger eller bedriftssensitiv informasjon. Slik bruk skal imidlertid begrenses og aller helst unngås.

- Nærmeste leder er ansvarlig for at tilgang til sensitiv informasjon følger prinsippet om tilgang i henhold til tjenstlig behov. All tilgang skal gis i henhold til definerte rutiner og kun i henhold til tjenstlig behov.

Opplæring

- Du skal ha gjennomgått nødvendig sikkerhetsopplæring i løpet av tre måneder etter ansettelse eller engasjement i NHN.

- Du er selv ansvarlig for å følge de regler som gjelder for bruk av de forskjellige informasjonssystemene, og for behandling av beskyttelsesverdig informasjon i henhold til gjeldende regler og krav definert i styringssystem for informasjonssikkerhet.

Brukernavn, passord og skjermsparer

- Du får tildelt brukernavn og passord av intern IKT og driftsansvarlig for tjenesten du skal ha tilgang til. Tilgang gis i henhold til fast rutine.

- Passord er strengt personlig og skal ikke oppgis til eller lånes ut til andre. Dette er et personlig ansvar.

- Passordet skal følge kravene gitt i styringssystem for informasjonssikkerhet.

- Dersom du har mistanke om at passordet har blitt kjent av uvedkommende, skal passordet byttes og hendelsen rapporteres som et avvik til sikkerhetsleder, snarest mulig.

- PC skal låses når arbeidsplassen forlates. Maskinen skal også være satt opp med automatisk skjermsparer med aktivering etter 15 minutters inaktivitet. Maskiner som ikke er underlagt et felles driftsregime, som for eksempel frittstående driftsmaskiner, skal settes opp med samme policy av bruker.

- Du skal alltid logge ut før du overlater maskinen til andre.

Oppdatering av antivirusprogram og operativsystem

- Oppdatering av antivirus og programvare/OS på klienter i kontornettet håndteres av intern IKT. For servere i NHN sin infrastruktur håndteres det av de respektive driftsteam. Hvis oppdatering krever omstart av maskinen, skal bruker så raskt som mulig gjennomføre dette.

Internett

- Brukere har tilgang til å benytte Internett samt sende og motta e-post fra sin lokale arbeidsstasjon/PC.

- Det er ikke tillatt å laste ned utuktig materiale, opphavsrettslig beskyttet materiale (f.eks. musikk, filmer og programvare) eller annet som er i strid med lovverket.

- Ressurskrevende tjenester, eksempelvis radiolytting og TV/video-streaming, skal begrenses for ikke å påvirke jobbrelatert trafikk i nettet negativt.

- NHN har anledning til å logge informasjon om Internett og e-post-trafikk for å sikre alminnelig drift, samt for sporing ved eventuelle sikkerhetsbrudd.

- Det er ikke tillatt å forsøke å forbigå sikkerhetsmekanismer beskrevet i denne sikkerhetsinstruks, for eksempel ved å skjule ikke-tillatte tjenester gjennom andre tjenester.

- Ved bruk av sosiale media skal bruker påse at det ikke deles informasjon om arbeidssted som kan oppfattes som sensitive.

E-post

- Dersom e-post må benyttes for overføring av beskyttelsesverdig informasjon, skal informasjonen sendes som kryptert vedlegg til e-post med godkjent krypteringsprogram. Passord til den krypterte filen skal sendes på et annet medium enn mail, f. eks. SMS.

- Brukere er selv ansvarlig for å vurdere hva som er arkivverdig. Ved tvil kan arkivansvarlig kontaktes.

Bærbar PC, mobil, nettbrett og annet portabelt utstyr

- PC, nettbrett og annet portabelt utstyr er i utgangspunktet styrt eller konfigurert av intern IKT. Dette oppsettet skal ikke endres av bruker.

- Beskyttelsesverdig informasjon skal ikke lagres på bærbar PC, nettbrett eller annet portabelt utstyr med mindre det er installert godkjente sikkerhetsløsninger (normalt med kryptert disk).

- Bærbar PC (jobb-PC) som benyttes som klient i NHN-nett, kan benyttes i forbindelse med jobb på reiser og hjemme. Jobb-PC skal ikke benyttes til annet enn jobbrelaterte oppgaver.

- Den enkelte bruker er ansvarlig for å håndtere bærbar PC og andre enheter med informasjon i henhold til sikkerhetskrav definert av NHN.

- La aldri bærbar PC, nettbrett eller annet bærbart utstyr ligge synlig uten tilsyn utenfor NHNs avsperrede områder.

Sikkerhetskopiering

- For å sikre at det blir tatt sikkerhetskopier skal all jobbrelatert informasjon lagres på, eventuelt kopieres til servere i NHN.

- For Jobb-PC som benyttes i forbindelse med reiser og hjemmearbeid, må oppdatering mot servere i NHN gjøres regelmessig, spesielt dersom andre er avhengig av informasjonen.
- Ved behov for gjenoppretting av sikkerhetskopiert informasjon, kontakt intern IKT eller driftsansvarlig for den tjenesten der behovet for gjenoppretting er.

Installasjon av programvare og maskinvare

- Det skal ikke benyttes programvare som avviker fra lisensavtaler til produsenter.

- All lisensiert programvare på maskinen skal godkjennes av intern IKT eller ansvarlig driftsteam. Dette gjelder alt utstyr.

- På klienter tilknyttet kontornettet tillates installasjon av privat programvare som f.eks. Spotify eller Wimp/Tidal for musikk. Annen programvare, som f. eks. spill tillates ikke. Intern IKT definerer hva som tillates.

- Dersom du har behov for ytterligere lisensiert programvare, ta kontakt med intern IKT eller ansvarlig driftsteam.

- All maskinvare og lagringsmedia/harddisk skal være registrert hos intern IKT eller ansvarlig driftsteam. Dersom dette mangler skal intern IKT eller ansvarlig driftsteam varsles.

Fjerntilgang

- Ekstern tilkopling mot NHN tillates kun etter godkjenning fra intern IKT eller ansvarlig driftsteam og kun gjennom godkjente løsninger.

Privat PC

- Kunde- eller NHN-informasjon tillates ikke lagret på privat PC. Det er ikke tillatt å koble utstyr som ikke tilhører NHN til virksomhetens nettverk. Unntaket er gjestenett.

Reparasjon, service og vedlikehold

- Alle feil eller mistanker om feil i informasjonssystemet (både maskinvare og programvare) skal snarest mulig rapporteres til intern IKT eller ansvarlig driftsteam.

- Det er kun intern IKT eller ansvarlig driftsteam som kan iverksette arbeid som utføres av eksternt personell på informasjonssystemer og utstyr.

Håndtering av informasjon og medier

Håndtering

- Dokumenter (papir, foiler etc.) og lagringsmedia, som CD, DVD og disketter, minnepinner etc., skal behandles iht. gjeldende rutiner fastsatt av virksomheten.

Kassering av medier

- Disker, utstyr som inneholder harddisker og annet lagringsmateriale (f.eks. minnebrikker, backup-tape etc.), skal leveres inn for forsvarlig destruksjon. Det finnes egne avtaler og rutiner for dette.

- Lagringsmedia som CD, DVD, minnepinner og disketter, etc.:
  - Personopplysninger skal leveres til intern IKT for destruksjon.

FYSISK ADGANG

Adgangskort

- Dersom du mister nøkkel/nøkkelkort, meld umiddelbart fra til administrasjonen eller sikkerhetsleder.

- Bruker som slutter eller går ut i permisjon, skal levere nøkkel/nøkkelkort tilbake til administrasjonen.

Besøkende

Den som mottar besøkende, er ansvarlig for at besøkende

- blir registrert i resepsjonen

- hentes i resepsjonen og følges tilbake av den som mottar besøket

- ikke oppholder seg i NHNs lokaler uten følge av en ansatt.

Besøk utenom ordinær arbeidstid skal begrenses.

KONTAKT MED MEDIA

Det er kun administrerende direktør, direktør for HR og kommunikasjon, eller den han/hun gir ansvaret til som har myndighet til å uttale seg til presse eller andre media i forbindelse med saker som gjelder IT-sikkerhet, sikkerhetsbrudd eller større hendelser.

NØDHJELP

Brann: Nødnummer 110
Håndslukkingsapparat CO2 og husbrannslange finnes i lokalene.
Brannalarm meldes automatisk til brannvesen.

Politi: Nødnummer 112
Ambulanse: Nødnummer 113
Vann:
Meld fra til administrasjonen.

PERSONELLSIKKERHET

Sikkerhetsinstruks og taushetserklæring
Bruker skal rette seg etter Sikkerhetsinstruks for brukere i Norsk Helsenett (dette dokumentet) og underskrive denne, samt taushetserklæring.

Konsekvenser ved brudd på retningslinjene
Konsekvenser for bruker som har forårsaket brudd på sikkerhetsreglene vil bli vurdert i hvert enkelt tilfelle, og kan ved alvorlige brudd føre til oppsigelse/avskjed, se virksomhetens reglement.

RAPPORTERING OG AVVIK

Rapportering av sikkerhetsbrudd/hendelser
Meld straks fra til sikkerhetsleder dersom du oppdager sikkerhetsbrudd eller hendelser som kan ha betydning for sikkerheten. Avvik skal meldes gjennom etablert avvikssystem, og melding sendes da automatisk til sikkerhetsleder.

AVVIKSHÅNDTERING

Avvik på denne instruks skal håndteres i henhold til avviksrutine og skal varsles til sikkerhetsleder umiddelbart.

Dersom brukere har behov som avviker fra denne instruks, skal det sendes en anmodning til sikkerhetsleder via nærmeste leder.

Sikkerhetsinstruksen er lest og akseptert:

Sted og dato: _____

Navn (blokkbokstaver): _____

Signatur: _____