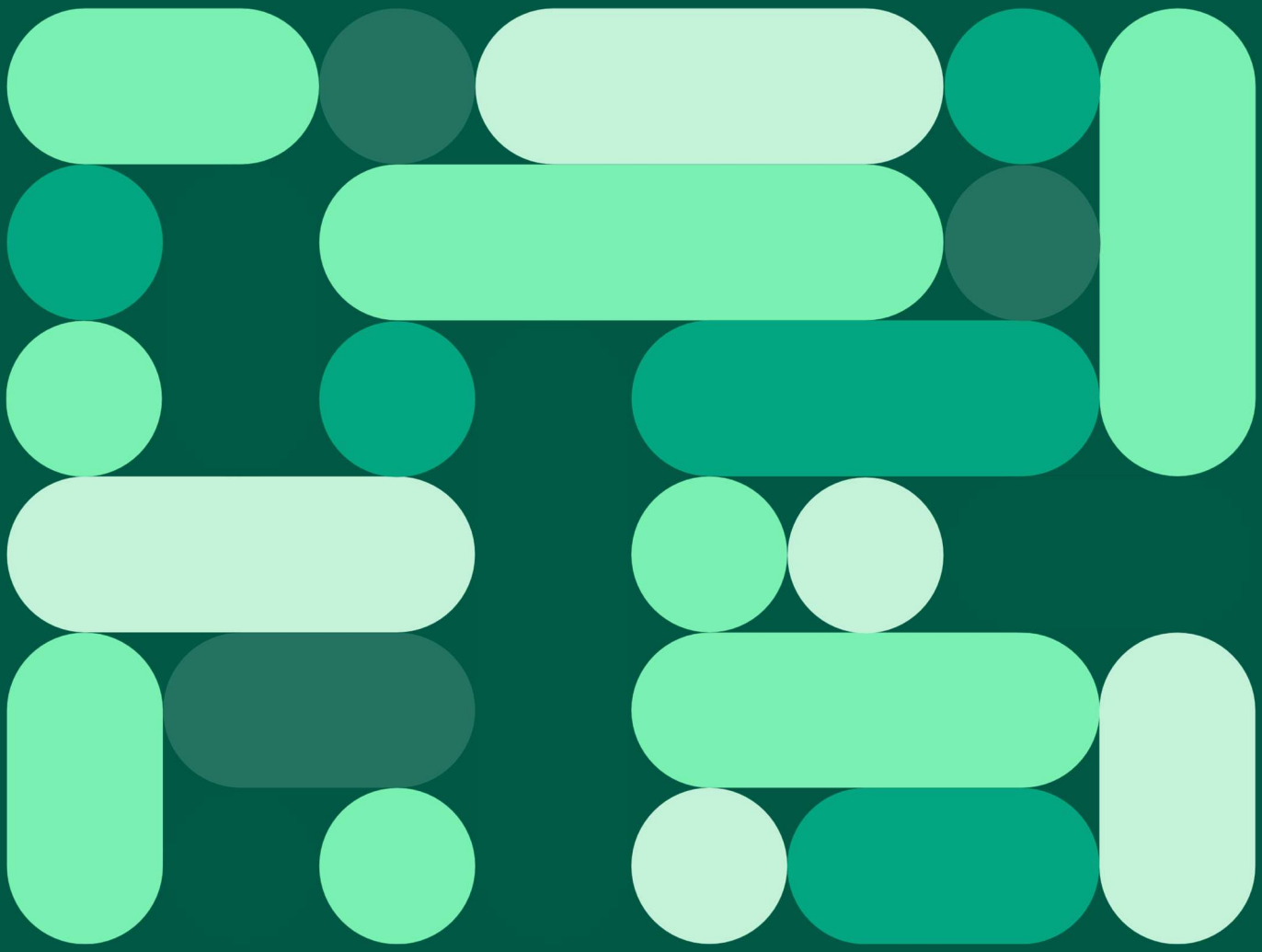

Retningslinjer for sikkerhet og personvern

01 Overordnet retningslinje for sikkerhet og personvern i NHN

Versjon 1.2

1 SIKKERHET OG PERSONVERN I NHN

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. NHN knytter helsetjenesten sammen og gjør helsedata og IKT-tjenester tilgjengelig for helseforvaltningen, helsepersonell, pasienter og befolkningen forøvrig – trygt og enkelt. NHN 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 NHN helseinformasjon og andre personopplysninger om hele Norges befolkning, i tillegg til virksomhetsinformasjonen til våre kunder og egen virksomhet. Tjenesteleveransene fra NHN 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, eksempelvis 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 tapt tillit i sektoren og i befolkningen, noe som igjen påvirker helsetjenestens evne til å utvikle nye digitale løsninger.

1.1 Mål for arbeidet med sikkerhet og personvern

Hovedmålene for arbeidet med sikkerhet, personvern og beredskap i NHN er å:

- Legge til rette for sikker og effektiv digital samhandling i helse- og omsorgssektoren. Sikkerhet og personvern skal være iboende egenskaper i alle tjenestene som utvikles og leveres fra NHN. NHN er en sikker og tygg tjenesteleverandør
- Ivareta sikker og stabil drift av kritiske IKT-tjenester, gjennom godt forebyggende sikkerhetsarbeid. Helsesektorens behandlingskapasitet og beredskapskapasitet skal ivaretas både i hverdagen og under nasjonale kriser. NHN er en beredt tjenesteleverandør.

- Sikre at helse- og personopplysninger forvaltes i henhold til lovpålagte krav og befolkningens rett til vern av privatlivet slik at NHN leverer menneskevennlige tjenester, og sikre etterlevelse av lovpålagte krav om å ivareta nasjonale sikkerhetsinteresser.

Som styrende prinsipp skal all utvikling, drift og forvaltning av tjenester og informasjonssystemer i NHN ta utgangspunkt i en risikobasert tilnærming. Dette danner grunnlag for effektiv håndtering av risiko gjennom implementasjon av risikoreduserende tiltak som skal sikre nødvendig grad av tilgjengelighet, integritet og konfidensialitet.

1.2 Målgruppe

Innholdet i dette dokumentet gjelder for alle forretningsområder, alle ansatte, midlertidige ansatte og vikarer i NHN, i tillegg til innleide konsulenter når de opptrer på vegne av NHN.

1.3 Overordnet organisering og oppfølging

Administrerende direktør i NHN har det overordnede ansvaret for sikkerhet og personvern, og er eier av denne retningslinjen. **Sikkerhetsdirektør** og sikkerhetsdivisjonen er ansvarlig for å koordinere og kontrollere etterlevelsen av denne retningslinjen i NHN, og å veilede organisasjonen til god etterlevelse gjennom kunnskapshevende og holdningsskapende arbeid. Alle **linjeledere** er ansvarlig for operasjonalisering og etterlevelse av denne retningslinjen i egen linje, slik at sikkerhet og personvern blir en integrert del av arbeidshverdagen og integrert i alle produkt og tjenesteleveranser fra NHN.

NHN sikrer planlagt og systematisk arbeidet med sikkerhet og personvern gjennom et styringssystem basert på bransjestandarden ISO 27001, kravene i Normen og NSMs grunnprinsipper for IKT-sikkerhet.

02 Retningslinje for organisering av sikkerhets- og personvernarbeidet

Versjon 1.6

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Denne retningslinjen beskriver roller eller funksjoner og tilhørende ansvar tilknyttet sikkerhet og personvern internt i NHN. Sektorvise funksjoner, slik som HelseCert, inngår ikke som del av NHNs interne styringssystem.

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

Tydelige roller eller funksjoner med tilhørende ansvar er en forutsetning for å ivareta sikkerhet og personvern i NHN. Den enkelte ansatte eller innleide, uavhengig av arbeidsoppgaver, har et ansvar for at sikkerhet og personvern ivaretas i NHN.

Særskilte roller eller funksjoner innen fagområdene sikkerhet og personvern, samt andre roller og funksjoner som er nødvendig for å ivareta tilfredsstillende nivå av sikkerhet og personvern, SKAL identifiseres. Rollens eller funksjonens myndighet SKAL samtidig fastsettes. Dette beskrives kort i tabellen under.

Veileder for organisering av sikkerhets- og personvernarbeidet beskriver typiske arbeidsoppgaver for disse rollene og funksjonene ytterligere, se referanser.

4.1 Retningslinje for organisering

Retningslinje	Beskrivelse
R02.1.1	Organisering av sikkerhets- og personvernarbeidet i NHN skal være tydelig definert gjennom tydelige beskrivelser av roller/funksjoner og ansvar
R02.1.2	Administrerende direktør i NHN skal ha det overordnede ansvaret for sikkerhet og personvern, og er eier av overordnet retningslinje for sikkerhet og personvern.
R02.1.3	Seksjon for sikkerhet og personvern skal være ansvarlig for å spesifisere obligatoriske retningslinjer og standarder i NHNs styringssystem for sikkerhet og personvern, koordinere og kontrollere etterlevelsen av disse, og å veilede organisasjonen til god etterlevelse gjennom kunnskapshevende og holdningsskapende arbeid.
R02.1.4	Sikkerhetshetsdirektøren skal sikre at det finnes funksjoner for å koordinere og etterleve arbeid med sikkerhet og personvern i NHN, og er eier av fagspesifikke retningslinjer og standarder
R02.1.5	Sikkerhetsleder skal lede, koordinere, kontrollere og veilede arbeidet innen ett eller flere fagområder i NHN, og jobber primært med styringsgrunnlag og retningslinjer
R02.1.6	NHN skal ha et personvernombud, som er virksomhetens uavhengige ressurs på personvernområdet. Personvernombudet skal lede og bidra i arbeidet med personvern og gi råd til ledelsen og andre i virksomheten, men også kontrollere etterlevelsen av regelverket, i tråd med kravene i lov om behandling av personopplysninger.
R02.1.7	Beredskapsfunksjonen skal sørge for at NHN har oppdatert beredskapsplanverk, at planverket er kjent og at det regelmessig planlegges og gjennomføres beredskapsøvelser. Beredskapsleder skal være ansvarlig for operativt nivå i krisesituasjoner
R02.1.8	Linjeledere på alle nivåer skal være ansvarlig for operasjonalisering og etterlevelse av obligatoriske retningslinjer i egen linje, slik at sikkerhet og personvern blir en integrert del av arbeidshverdagen og integrert i alle produkt- og tjenesteleveranser fra NHN, gjennom hele livsløpet (f.eks. utvikling, drift, forvaltning).

4.2 Retningslinje for organisering underlagt sikkerhetsloven

Retningslinje	Beskrivelse
R02.2.1	Det skal utpekes en sikkerhetsleder og en stedfortredende sikkerhetsleder som har det faglige ansvaret knyttet til sikkerhetsloven.
R02.2.2	Datasikkerhetsleder skal utnevnes i tilknytning til fysisk lokasjon der dette kreves
R02.2.2	Administrerende direktør har delegert autorisasjonsansvar til sikkerhetsleder og beredskapsdirektør

03

Retningslinje for programvaresikkerhet og innebygd personvern

Versjon 1.2

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Denne retningslinjen gjelder all programvareutvikling som skjer internt i NHN og som NHN har ansvaret for eksternt, herunder NHN sin rolle som leverandør. All anskaffelse, utvikling, videreutvikling og vedlikehold av programvare er omfattet. For utvikling av informasjonssystemer som er underlagt sikkerhetsloven kan egne krav gjelde.

Programvareutvikling omhandler systematisk design, programmering, testing og vedlikehold av programvare. I NHN kan programvareutvikling være løsninger som for eksempel Kjernejournal, eResept, Helsenorge.no eller en intern saksbehandlingsløsning som SMAX. Script til automatisering av infrastruktur og koding av retningslinje vurderes ikke som programvareutvikling.

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

Denne retningslinjen setter krav til programvaresikkerhet og innebygd personvern ved programvareutvikling og forvaltning av drift og tjenester, slik at informasjonssystemene er sikre, robuste og ivaretar de registrertes rettigheter og friheter gjennom hele livsløpet.
Denne retningslinjen gjelder uavhengig av hvilken utviklingsmetodikk som benyttes. Krav i denne retningslinjen er også gjeldende for eksterne leverandører og utkontraktert utvikling med mindre andre krav er avtalt mellom NHN og leverandøren.

4.1 Retningslinje for programvaresikkerhet og innebygd personvern

Retningslinje	Beskrivelse
R03.1.1	Innebygd sikkerhet og personvern skal inngå i prosesser for programvare- og systemutvikling. Dette arbeidet skal være forankret i risikostyring, se referanse 8
R03.1.2	Det skal være etablert og vedlikeholdt en sikkerhetsarkitektur som ivaretar behov for et sikkert og motstandsdyktig IKT-system.
R03.1.3	Alle komponenter i en løsning, produkt eller verdikjede skal sikkerhetsmessig fungere godt sammen og ivareta definert sikkerhetsnivå.
R03.1.4	Bruk separate miljøer for utvikling, test og produksjon for å sikre tilstrekkelig separasjon mellom miljøene, slik at operative virksomhetsprosesser ikke blir påvirket av feil i andre miljøer.
R03.1.5	NHN skal sikre at data som benyttes til utviklings- og testformål ikke inneholder personopplysninger.
R03.1.6	NHNs utviklingsprosesser skal ta særskilt høyde for å ivareta krav til sikkerhet i løsninger der informasjon om personer med adressesperre (Fortrolig og strengt fortrolig) utvikles, etter retningslinjer i Normen (Se referanse 7)
R03.1.7	Det skal utføres tilstrekkelig med sikkerhetstesting som en del av utviklingsprosessen for å verifisere sikkerhetsfunksjonalitet og lukke sårbarheter.
R03.1.8	Ved bruk av kode fra eksterne kilder (bibliotek, rammeverk, «toolkits» med mer) skal det regelmessig, og fortrinnsvis automatisk, sjekkes for sårbarheter og kontrollert oppdateres til nye versjoner. Dette gjelder både for offentlig tilgjengelig («open source») og kommersiell kode

4.2 Retningslinje for programvaresikkerhet og innebygd personvern i prosjekter

Retningslinje	Beskrivelse
R03.2.1	Retningslinje i avsnitt 4.1 gjelder også for prosjekter og skal være tydelig beskrevet i prosjektmetodikken
R03.2.2	Prosjektmodellen i NHN skal spesifisere dedikert budsjettering for finansielle midler til gjennomføring av sikkerhets- og personvernaktiviteter gjennom prosjektets livssyklus.

04 Retningslinje for risikostyring av informasjonssikkerhet

Versjon 1.3

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Omfanget av retningslinjen for risikostyring av informasjonssikkerhet er alle tjenester, registre og informasjonssystemer som leveres, driftes eller forvaltes av NHN. Retningslinjen gjelder også interne informasjonssystemer, og tjenester som er omdømmemessig viktig for NHN.

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

Risikostyring av informasjonssikkerhet og personvern skal bidra til at NHN på en systematisk måte kan forutse, forebygge og redusere sannsynligheten for, og konsekvensen av, uønskede hendelser relatert til informasjonsbehandlingen og tjenestene vi leverer. Målrettet risikostyring mot et oppdatert trusselbilde skal være en innebygd del av organisasjonen.

4.1 Retningslinje for risikostyring

Retningslinje	Beskrivelse

R04.1.1	NHN skal fastsette nivå for akseptabel risiko i virksomhetens informasjonssystemer gjennom akseptkriterier.
R04.1.2	Alle informasjonssystemer som leveres, driftes eller forvaltes av NHN, og systemer som er omdømmemessig viktig for NHN, skal opprettholde nivå for akseptabel risiko gjennom definert prosess for risikostyring.
R04.1.3	Alle tjenester, registre og informasjonssystemer skal ha en definert risikoeier.
R04.1.4	Risikoeier skal sørge for at risiko rapporteres regelmessig til virksomhetens ledelse.
R04.1.5	Risikostyring og risikonivå skal dokumenteres. Dokumentasjon inkluderer risikovurderinger, eierskap, sporbare beslutninger, sikkehetsavvik og plan for å oppnå akseptabel risiko.
R04.1.6	NHNs ledelse skal jevnlig følge opp virksomhetens risikonivå med formål å drive forsvarlig virksomhetsstyring.

05 Retningslinje for aktiva og klassifisering

Versjon 1.3

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Omfanget av retningslinjen er *aktiva* som eies av NHN, eller som NHN gjennom leverandørrolle er ansvarlig for eksternt. Deler av retningslinjen gjelder også for *skjermingsverdig* informasjon, informasjonssystemer eller objekter som faller innenfor sikkerhetsloven.

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

3. Faglig innhold

Som leverandør av infrastruktur og nasjonale e-helseløsninger, og i sin rolle som arbeidsgiver, besitter NHN en rekke aktiva. Denne retningslinjen inneholder krav til oversikt og eierskap over aktivaene.

Informasjon som behandles i NHN er av forskjellig kritikalitet og sensitivitet. For å sikre effektiv og forsvarlig sikring av informasjon og informasjonssystemer inneholder denne retningslinjen krav til klassifisering.

4.1 Retningslinje for aktiva

Retningslinje	Beskrivelse
R05.1.1	NHN skal føre en oversikt over tjenester og tilhørende informasjonssystemer. Oversikten skal beskrive tjenestekritikalitet, eierskap og informasjonstyper for alle informasjonssystemer.
R05.1.2	NHN skal føre et register over alle maskin- og programvare komponenter som utgjør tjenester i drift. Registeret skal beskrive status og komponentenes relasjon og avhengighet til hverandre

4.2 Retningslinje for aktiva underlagt sikkerhetsloven

Retningslinje	Beskrivelse
R05.2.1	Det skal føres oversikt over hvilke dokumenter som oppbevares hos NHN, og som i henhold til sikkerhetsloven er sikkerhetsgradert.
R05.2.2	Sikkerhetsnivået for NHNs arkivsystem og oppbevaringsløsninger for sikkerhetsgradert informasjon skal være tilpasset sikkerhetsgrad KONFIDENSIELT.
R05.2.3	Informasjon som er gradert høyere enn KONFIDENSIELT skal ikke behandles i virksomheten.
R05.2.4	Informasjon med sikkerhetsgrad BEGRENSET skal kun behandles av autorisert personell. Informasjon med sikkerhetsgrad KONFIDENSIELT skal kun behandles av sikkerhetsklarert og autorisert personell, i sikret område.
R05.2.5	Dersom en tjeneste eller infrastruktur er utpekt og klassifisert som skjermingsverdig objekt eller infrastruktur skal sikring av tjenesten følge kravene gitt i sikkerhetsloven.

4.3 Retningslinje for klassifisering

Retningslinje	Beskrivelse
R05.3.1	All informasjon som NHN forvalter og behandler skal kategoriseres i informasjonstyper og klassifiseres i henhold til lovkrav og sensitivitet for å sikre konfidensialitet og integritet.
R05.3.2	Informasjonstyper og tilhørende sikkerhetsklasser skal være beskrevet og gjort tilgjengelig som hjelpemiddel for alle ansatte og innleide.
R05.3.3	Alle informasjonssystemer i NHN skal klassifiseres etter tjenestekritikalitet, og behov for å ivareta konfidensialitet, integritet og tilgjengelighet i henhold til identifisert risiko.

06 Retningslinje for sikkerhet i drift og forvaltning

Versjon 1.3

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Retningslinjen dekker sikkerhet i operasjonell drift knyttet til følgende områder:

- Oversikt over utstyr, tjenester og ansvar
- Beskyttelse av informasjon og informasjonssystemer
- Logging
- Arkitektur
- Sårbarhetstesting

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

Sikkerhet i operasjonell drift er avgjørende for å sikre de dataene vi behandler både på vegne av oss selv og våre *kunder*.

4.1 Retningslinje for sikkerhet i operasjonell drift

Retningslinje	Beskrivelse
R06.1.1	NHN skal sikre at informasjon og systemer har tilstrekkelig sikkerhet for å ivareta integritet, konfidensialitet og tilgjengelighet i henhold til vedtatt risikoaksept.
R06.1.2	NHN skal sørge for at informasjon og informasjonssystemer er beskyttet mot skadevare og ondsinnede angrep.
R06.1.3	NHN skal sikre at systemer til enhver tid er oppdatert og oppgradert.
R06.1.4	NHN skal sørge for at alt utstyr, tjenester og programvare logger i henhold til loggkrav fastsatt i egen standard.
R06.1.5	NHN skal ha sentralisert logginnsamling, monitorering og sikkerhetsovervåkning av logger for å kunne feilsøke effektivt, og bidra til å oppdage inntrengingsforsøk og uautorisert bruk av informasjonssystemer.
R06.1.6	NHN skal dokumentere og ha kontroll over programvaren og infrastruktur som er i bruk i virksomheten for å være trygg på at den overholder krav til sikkerhet og personvern. Dette gjelder både programvare og infrastruktur som installeres lokalt, og i skytjenester som tas i bruk.
R06.1.7	NHN skal ha systemer for å identifisere og detektere sårbarheter i teknisk infrastruktur.
R06.1.8	NHN skal sikre at det ikke ligger igjen virksomhetskritisk informasjon eller personopplysninger som kan komme på avveie ved avhending av utstyr.
R06.1.9	NHN skal dokumentere hvordan sikkerhet og personvern sikres i tjenestene gjennom å beskrive hvordan konfidensialitet, integritet og tilgjengelighet ivaretas.
R06.1.10	NHN skal gjennomføre inntrengningstester mot egne tjenester og infrastruktur ved større endringer, og eller minimum en gang per år.
R06.1.11	NHN skal håndtere endringer knyttet til operasjonell drift gjennom en etablert endringsprosess

07 Retningslinje for fysisk sikkerhet

Versjon 1.4

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Retningslinjen setter krav til hvilke tiltak som er påkrevet for å sikre tilstrekkelig fysisk sikkerhet der:

- NHN behandler informasjon
- informasjon behandles på vegne av Norsk Helsenett
- NHN behandler informasjon på vegne av andre

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

4.1 Retningslinje for fysisk sikkerhet

Retningslinje	Beskrivelse
R07.1.1	NHN skal forhindre at uautorisert personell kan ta seg inn på områder hvor det er fare for at de kan få tilgang til, eller volde skade på informasjon eller informasjonssystemer.
R07.1.2	Tilgang til NHNs lokaler skal kun gis til personell med tjenstlig behov, og tilgang skal logges. Loggene skal kunne hentes ut ved behov.

R07.1.3	NHN skal ha etablerte rutiner og tiltak som hindrer uautorisert tilgang til ubevoktet utstyr
R07.1.4	NHN skal sikre at driftsomgivelsene der informasjon og informasjonssystemer plasseres har tilstrekkelig beskyttelse mot uønskede fysiske hendelser knyttet til: • Strømstans • Brann • Vannskade • Manglende kjøling • Uautorisert tilgang
R07.1.5	NHN skal gjøre en vurdering av redundans eller alternative lokaler for drift der tjenester som i henhold til kritikalitet krever høy oppetid.
R07.1.6	NHN skal sikre at informasjon og informasjonssystemer som er gradert eller underlagt krav til objektsikring beskyttes i egnede områder i henhold til kravene i Sikkerhetsloven.
R07.1.7	NHN skal etablere løsninger som sikrer mot uautorisert tilgang til data hvis mobilt utstyr eller bærbare medier havner på avveie.
R07.1.8	NHN skal ha rutiner og avtaler som sikrer at lagringsmedier slettes forsvarlig før de sendes til service. Hvis sletting ikke er mulig skal utstyret kun sendes til leverandør der NHN har tegnet tilstrekkelige databehandleravtale.
R07.1.9	NHN skal gjennom rutiner og avtaler sørge for at utstyr som avhendes slettes eller destrueres på en slik måte at data ikke kan gjenskapes.
R07.1.10	Adgangskort med bilde skal bæres synlig så lenge man oppholder seg i NHNs lokaler. Gjelder ansatte, innleide og eksterne med fast tilgang.
R07.1.11	Alle besøkende skal bære lånekort eller ha navnelapp synlig så lenge de oppholder seg i NHNs lokaler. Den ansatte skal ha kontroll på sine besøkende under oppholdet. Lånekort skal leveres tilbake ved endt besøk.
R07.1.12	NHN skal ha rutiner for å håndtere uvedkommende i NHNs lokaler.

08 Retningslinje for avviksbehandling

Versjon 1.4

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Retningslinjen dekker kravene til avvikssystem og prosess for avvikshåndtering.

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

Et avvik knyttet til informasjonssikkerhet eller personvern er en hendelse, eller mulig hendelse, som berører vår evne til å direkte eller indirekte sikre opplysninger i forhold til konfidensialitet, integritet eller tilgjengelighet. Avvik kan være:

- Brudd på gjeldende rutiner eller regelverk
- Hendelser som kan ha konsekvenser for informasjonssikkerheten vår
- Utført av ansatte, som brudd på sikkerhetsbestemmelser (bevisst eller ubevisst)
- Utført av eksterne, som fysisk innbrudd eller elektroniske angrep
- Brudd på personopplysningssikkerheten.

Avvik gjelder både interne systemer/forhold, og avvik som oppstår i tjenestene vi drifter eller utvikler.

4.1 Retningslinje for avviksbehandling

Retningslinje	Beskrivelse
R08.1.1	NHN skal ha et avvikssystem og tilhørende rutiner for oppfølging av avvik knyttet til sikkerhet og personvern.
R08.1.2	Alle ansatte og innleide skal få relevant opplæring slik at de er i stand til å kjenne igjen og innrapportere situasjoner som kan innebære et avvik knyttet til sikkerhet og personvern
R08.1.3	Alle ansatte, innleide og relevante tredjeparter skal umiddelbart registrere sak i avvikssystemet når de oppdager eller har mistanke om et avvik.
R08.1.4	Avvik skal følges opp i hver enkelt divisjon, og divisjonsdirektør har det overordnede ansvaret for avviksoppfølging i egen divisjon.
R08.1.5	Personvernombudet skal informeres umiddelbart ved mistanke om brudd på personopplysningssikkerheten.
R08.1.6	Når NHN er dataansvarlig skal brudd på personopplysningssikkerhet meldes til Datatilsynet innen 72 timer hvis det medfører risiko for rettigheter og friheter for den/de det gjelder. Dersom NHN er databehandler skal mistanke eller brudd på personopplysningsikkerheten meldes til dataansvarlig uten ugrunnet opphold.
R08.1.7	Kripos skal varsles ved uberettiget tilgang til geolokaliserende opplysninger og opplysninger om adresser som er beskyttet med adressesperre i folkeregisteret som angir at opplysningene er fortrolige eller strengt fortrolige.
R08.1.8	Linjeleder skal etablere en tiltaksplan for å lukke innmeldte avvik, og med en prioritering som hensyntar avvikets kritikalitet.
R08.1.9	Avvik som utgjør en høy operasjonell risiko, og som kan utnyttes av eksterne trusselaktører til å gjennomføre ondsinnede handlinger skal lukkes fortløpende.

09 Retningslinje for personellsikkerhet

Versjon 1.4

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Omfanget av retningslinjen for personellsikkerhet er alle midlertidige og fast ansatte, vikarer og innleide konsulenter i Norsk Helsenett. Deler av retningslinjen kan omfatte besøkende av NHNs lokaler, og personell hos NHNs leverandører.

Retningslinjen omfatter ikke krav som ivaretar ansattes eller innleides fysiske sikkerhet. Det henvises til Norsk Helsenetts HMS-dokumenter hvor disse kravene ivaretas.

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

Krav til personellsikkerhet skal ivaretas gjennom hele livsløpet
for ***ansettelsesforhold*** og ***oppdragsforhold;*** før, under, og ved endring og avslutning av arbeidsforhold. NHN skal ha etablerte prosesser for dette.

4.1 Retningslinje for personellsikkerhet

Retningslinje	Beskrivelse
R09.1.1	HR funksjonen skal sørge for at det utføres ID-sjekk og referansesjekk av kandidater før ansettelsesforhold med NHN etableres. Linjeleder har ansvaret for ID-sjekk av konsulenter.
R09.1.2	Ansatte skal signere og akseptere taushetserklæring og sikkerhetsinstruks før det gis tilgang til NHNs informasjon eller informasjonssystemer. Dokumentene er koblet sammen med arbeidsavtalen og skal arkiveres i NHN sitt arkivsystem.
R09.1.3	Innleide skal signere og akseptere taushetserklæring og sikkerhetsinstruks før det gis tilgang til NHNs informasjon eller informasjonssystemer. Dokumentene skal arkiveres i NHN sitt arkivsystem.
R09.1.4	Personer uten arbeidsavtale som gis midlertidig tilgang til NHNs informasjon og informasjonssystemer, skal signere taushetserklæring og sikkerhetsinstruks før tilgang til informasjonen gis
R09.1.5	Ved brudd på taushetserklæring eller sikkerhetsinstruks skal nærmeste leder varsle HR. Leder vurderer videre aksjon i samråd med HR og juridisk, i henhold til Lederhåndbok.
R09.1.6	Ved rekruttering og ansettelse til roller definert som kritiske så skal NHN gjennomføre bakgrunnssjekk og sikkerhetssamtale, og utfallet av disse være vurdert som innenfor akseptabelt risikonivå før ansettelsesforholdet kan starte.

4.2 Retningslinje for personellsikkerhet mtp Sikkerhetsloven

Retningslinje	Beskrivelse
R09.2.1	Alle ansatte og innleide, inkludert personell hos leverandør eller underleverandør, som gis tilgang til sikkerhetsgradert informasjon på nivå BEGRENSET skal være autorisert av Norsk helsenett. Alle ansatte og innleide, inkludert personell hos leverandør eller underleverandør, som gis tilgang til sikkerhetsgradert informasjon på nivå KONFIDENSIELL eller høyere skal være sikkerhetsklarert og autorisert i henhold til Sikkerhetsloven.
R09.2.2	Ansatte og innleid personell, inkludert personell hos underleverandører, som skal jobbe med skjermingsverdige tjenester, objekter eller infrastruktur, som definert i Sikkerhetsloven, skal sikkerhetsklareres eller adgangsklareres, og autoriseres på tilstrekkelig nivå.

10

Retningslinje for sikkerhet og personvern i anskaffelser og kontraktsoppfølgning

Versjon 1.4

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Retningslinjen gjelder for anskaffelser av IT-relaterte tjenester eller programvare som NHN anskaffer (kjøp eller gratis) og for de valgte leverandører som skal kunne aksessere, lagre, overføre eller på annen måte behandle NHNs informasjon. Retningslinjen omfatter hele anskaffelsesprosessen, fra planlegging og gjennomføring av anskaffelsen og gjennom kontraktens livsløp med oppfølging av avtalte leveranser frem til avslutning av leverandørforholdet.

Retningslinjen gjelder ikke for varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser.

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

4.1 Retningslinje for sikkerhet og personvern i anskaffelser og kontraktsoppfølging

Retningslinje	Beskrivelse
R10.1.1	NHN skal sørge for at informasjonssikkerhet og personvern ivaretas i alle anskaffelser.

R10.1.2	NHN skal etablere og vedlikeholde oversikt over alle avtaler og leverandører.
R10.1.3	NHN skal ha prosesser som sikrer at krav til informasjonssikkerhet og personvern i leverandørforhold og anskaffelser ivaretas i hele livsløpet til anskaffelsen og avtaleforholdet.
R10.1.4	NHN skal ha oversikt over hele leverandørkjeden, inkludert underleverandører av NHNs leverandører.
R10.1.5	Hver divisjon skal følge opp at deres leverandører og underleverandører etterlever krav til informasjonssikkerhet og personvern i anskaffelsen og avtalen.

11 Retningslinje for kryptografi

Versjon 1.4

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Retningslinjen gjelder for alle digitale tjenester levert og tatt i bruk av Norsk Helsenett, og skal etterleves av alle organisasjonsenheter som utvikler, drifter eller forvalter digitale løsninger.

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

Denne retningslinjen setter minimumskrav til bruk av kryptering og kryptoorganisasjon i Norsk Helsenett.

4.1 Retningslinje for kryptografi

Retningslinje	Beskrivelse

R11.1.1	Kryptonøkler har prinsipielt samme skjermingsverdi som den samlede verdien av informasjonen og informasjonssystemene de beskytter. Valg av nøkkellengder, kryptoprotokoller og krypteringsmekanismer skal hensynta verdien av informasjonen og informasjonssystemene de skal bidra til å sikre.
R11.1.2	Kryptomateriell skal kun forvaltes av autorisert personell, og lagres på tilstrekkelig sikrede og tilgangskontrollerte områder
R11.1.3	Kryptering skal benyttes når personopplysninger overføres eller når tilliten til informasjonskanalen er lav. For de ulike kanalene må det bestemmes på hvilket nivå krypteringen gjennomføres (for eksempel i applikasjonen/transportlaget, på nettverkslaget eller på datalinklaget) etter en risikobasert tilnærming
R11.1.4	Alle trådløse nettverksforbindelser i, og levert av, Norsk helsenett skal krypteres.
R11.1.5	Kryptering av lagrede data skal vurderes som et sikringstiltak og behovet skal vurderes i en risikovurdering.
R11.1.6	Endepunktsutstyr eid av Norsk helsenett skal utstyres med sertifikater eller krypteringsnøkler for å oppnå autentisering av endepunktet, og som mekanisme for å oppnå transportkryptering.
R11.1.7	Kryptering skal følge oppdaterte, anerkjente og robuste standarder, basert anbefalinger fra Nasjonal Sikkerhetsmyndighet (NSM Cryptographic Recommendations).
R11.1.8	Programvare, biblioteker og maskinvare som tas i bruk til krypto-formål bør være sertifisert i henhold til anerkjente standarder (slik som FIPS 140-2).
R11.1.9	Kryptonøkler og sertifikater skal forvaltes aktivt og ha en begrenset levetid. Kryptonøkler og sertifikater skal skiftes ut etter den definerte levetiden, og det skal være mekanismer for å kunne bytte/rotere nøkler
R11.1.10	Kryptoalgoritmer og nøkler skal kunne byttes ut, for eksempel dersom algoritme eller nøkler blir kompromittert.
R11.1.11	Norsk helsenett bør ha én felles kryptoforvaltningsfunksjon som er ansvarlig for forsvarlig nøkkeladministrasjon for alle informasjonssystemer og tjenester som er utviklet og levert av Norsk helsenett. Kryptoforvalningsfunksjonen bør både ha ansvar for intern nøkkelforvaltning, og sertifikater kjøpt i markedet.

12 Retningslinje for brukeradministrasjon og tilgangskontroll

Versjon 1.3

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Retningslinje for brukeradministrasjon og tilgangskontroll gjelder all informasjonsbehandling som skjer internt i NHN og som NHN har ansvaret for eksternt, herunder NHN sin rolle som leverandør.

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

Retningslinjen setter krav til brukeradministrasjon og tilgangskontroll for alle informasjonssystemer NHN forvalter. Kravene gjelder for de som administrerer brukertilganger i NHN, for alle som har fått en bruker i NHN og alle system som NHN.

4.1 Retningslinje for brukeradministrasjon

Retningslinje	Beskrivelse
R12.1.1	NHN skal ha dokumenterte prosesser for brukeradministrasjon. Dette inkluderer dokumenterte prosesser for å opprette, endre, deaktivere og slette brukerkontoer.

R12.1.2	Alle personlige brukerkontoer i NHN skal knyttes til en bestemt person.
R12.1.3	Alle ikke-personlige kontoer skal være unike, og kontoene skal være knyttet til en bestemt team/seksjon.
R12.1.4	Alle brukere i NHN skal ha unike kombinasjoner av brukernavn og passord.
R12.1.5	Det skal foreligge en dokumentert og sikker prosess for formidling av brukernavn og passord.
R12.1.6	Privilegert tilgang til produksjonsløsninger skal styres gjennom løsninger for privilegert tilgangsstyring. Dette skal sikre nødvendig kontroll og sporbarhet i bruken av de utvidede rettighetene som følger privilegerte brukerkontoer
R12.1.7	NHN skal ha oversikt over hvilke brukere som har tilgang til informasjonssystemer, og hvilke tilgangsrettigheter de har.
R12.1.8	Alle aktiviteter knyttet til brukeradministrasjon og tilgangskontroll skal logges slik at man blant annet sikrer sporbarhet på hvem som har godkjent en aktivitet, hva som er utført og når aktiviteten ble gjennomført. Tilgangsrettigheter skal dokumenteres i et autorisasjonsregister.
R12.1.9	Risikoeier skal gjennomføre egenkontroll av brukere og brukernes tilganger minimum en gang i året. Egenkontrollen skal sikre tilganger følger tjenstlig behov, og at tilganger til ansatte og innleid personell blir fjernet etter endt arbeids- eller kontraktsforhold. Kontrollaktiviteten skal dokumenteres.

4.2 Retningslinje for tilgangskontroll

Retningslinje	Beskrivelse
R12.2.1	Som hovedregel skal informasjon i NHN være tilgjengelig for alle ansatte og innleide, og kunne deles internt via NHNs samhandlingsløsninger. Informasjon som i henhold til informasjonsklassifisering har skjermingsverdi skal lagres på tilgangskontrollerte lagringsområder eller i tilgangskontrollerte informasjonssystemer.
R12.2.2	Alle tilganger til informasjonssystemer skal baseres på tjenstlig behov.
R12.2.3	Informasjonssystemer bør integreres med sentral katalogtjeneste for å forenkle brukeradministrasjonen, og sikre at tilganger til alle informasjonssystemer kan kontrolleres, og ved behov sperres, fra sentral kilde.
R12.2.4	NHN skal ha tydelige krav til passord, passordhvelv, engangskoder, og hvordan de skal håndteres.
R12.2.5	All tilgang til informasjonssystemer som inneholder informasjon klassifisert som intern/virksomhetskritisk, og som er publisert på internett skal være beskyttet med multi-faktor autentisering.
R12.2.6	Linjeledere skal sørge for at ansattes og innleides tilganger blir tilbaketrukket ved endring eller opphør av ansettelsesforhold eller innleieperiode.

4.3 Retningslinje for brukeradministrasjon og tilgangskontroll der NHN utfører brukeradministrasjon på vegne av kunder

Retningslinje	Beskrivelse
R12.3.1	Som hovedregel skal NHNs retningslinje for brukeradministrasjon og tilgangskontroll følges, med mindre kunden har instruert NHN om annen praksis.
R12.3.2	NHN skal ha oversikt over hvilke ansatte og innleide som har tilgang til infrastruktur med kundedata, og hva slags tilganger de har til kundens informasjon og informasjonssystemer. Denne informasjonen skal kunne oversendes kunde på forespørsel.
R12.3.3	Der NHN har et ansvar i kundens brukeradministrasjon skal NHN ha oversikt over hvilke brukere hos kunden som har tilgang til kundens informasjonssystemer, og hvilke tilgangsrettigheter de har. Denne informasjonen skal kunne oversendes kunde på forespørsel, slik at de kan gjennomføre nødvendig revisjon av brukere og tilgangsrettigheter. NHN gjennomfører ikke på selvstendig grunnlag revisjon av kundens brukere og deres tilganger til kundens informasjonssystemer

13 Retningslinje for hendelseshåndtering, beredskap og kontinuitetsplanlegging

Versjon 1.3

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Denne retningslinjen gjelder alle produkter og tjenester som ut fra en konsekvensvurdering er definert som kritiske for virksomheten.

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

Norsk helsenett skal sørge for at produkter og tjenester møter krav til konfidensialitet, integritet og tilgjengelighet. Denne retningslinjen skal sikre at NHN har beredskapsplanverk for virksomheten, samt kontinuitetsplan og gjenopprettingsplan for alle produkter og tjenester som ut fra en konsekvensvurdering (BIA - business impact analysis) er definert som kritiske for virksomheten.

Norsk helsenett skiller mellom major incidents (alvorlige IKT-hendelser, som håndteres gjennom kontinuitetsplanverket) og kriser (som utløser beredskapsplanverket). Det kan være tilfeller hvor en major incident over tid eskalerer til å bli en krise, og derfor utløser beredskapsplanverket. En krise kjennetegnes ved at det er en situasjon som stiller så høye krav at organisasjonens normale rutiner og ressurser ikke strekker til.

Kontinuitetsplanleggingen skal legge til rette for at kritiske virksomhetsprosesser vil fortsette innenfor akseptable nivåer når uønskede hendelser inntreffer, og ivareta NHNs evne til å håndtere major incidents og kriser på en effektiv, sikker og systematisk måte.

4.1 Retningslinje for beredskap og kontinuitetsplanlegging

Retningslinje	Beskrivelse
R13.1.1	NHN SKAL gjøre en kritikalitetsvurdering, også kjent som BIA (Business Impact Analysis). Kritikalitetsvurderingen SKAL inkludere både en overordnet vurdering på virksomhetsnivå og kritikalitetsvurderinger av produkter og tjenester som på virksomhetsnivå er definert med kritikalitet høy og kritisk (ihht til standard for klassifisering og tjenestekritikalitet, se referanse 5).
R13.1.2	NHN SKAL etablere kontinuitetsplan og gjenopprettingsplan for håndtering av major incidents og major security incidents tilknyttet produkter og tjenester som i kritikalitetsvurderingen på virksomhetsnivå er definert med kritikalitet høy og kritisk.
R13.1.3	NHN skal etablere beredskapsplanverk for håndtering av kriser. Beredskapsplanverket skal definere roller og ansvar og gi krav for organisering i en krise.
R13.1.4	NHN skal gjennomføre øvelser på beredskapsplanverk og kontinuitets- og gjenopprettingsplaner. Det skal øves på alle nivåer av kriseorganisasjonen (strategisk, operativt og taktisk). Øvelser skal evalueres og det skal utarbeides tiltak til forbedring.
R13.1.5	NHN SKAL gjennomføre test av gjenoppretting for produkter og tjenester som i kritikalitetsvurderingen på virksomhetsnivå er definert med kritikalitet høy og kritisk. Tester skal evalueres og det SKAL utarbeides tiltak til forbedring.

4.2 Retningslinje for incident management

Retningslinje	Beskrivelse
R13.2.1	NHN skal ha en prosess for incident management. Målet med prosessen er å gjenopprette normal drift så raskt som mulig ved incidents og security-incidents.

14 Retningslinje for samsvar og kontrollaktiviteter

Versjon 1.4

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, og leverandør av fellestjenester til helseforvaltningen, og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Retningslinje for samsvar og internkontroll gjelder for hele NHN, og alle tjenester, registre og *informasjonssystemer.* Retningslinjen gjelder også interne informasjonssystemer, og tjenester som er omdømmemessig viktig for NHN.

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

Denne retningslinjen skal bidra til at Norsk Helsenett gjennomfører kontrollaktiviteter som skal gi innsikt i selskapets etterlevelse krav i styringssystem for sikkerhet og personvern.

4.1 Retningslinje for samsvar og internkontroll

Retningslinje	Beskrivelse
R14.1.1	NHN skal sikre etterlevelse av gjeldende regelverk for informasjonssikkerhet og personvern knyttet til NHN sine tjenesteleveranser

R14.1.2	NHN skal sikre etterlevelse av sikkerhets- og personvernkrav vi har forpliktet oss til gjennom etablerte kontrakter, knyttet til tjenesteleveransene og forvaltning av data
R14.1.3	Sikkerhetsdivisjonen skal gjennomføre internkontroll av linje, med formål om å oppdage avvik fra etablerte retningslinjer i styringssystemet.

15 Retningslinje for behandling av personopplysninger

Versjon 1.2

1. Hensikt

Norsk helsenett SF (NHN) er nasjonal tjenesteleverandør på e-helseområdet, leverandør av fellestjenester til helseforvaltningen og skal legge til rette for sikker, personvernvennlig og effektiv elektronisk samhandling i helse- og omsorgssektoren. Hensikten med denne retningslinjen er å gi overordnede føringer for behandling av personopplysninger i Norsk Helsenett (NHN) slik at NHN kan sikre verdien personopplysninger for egen og kunders virksomhet og sørge for at personvernet til innbyggerne blir ivaretatt ved behandling av personopplysninger. I tillegg til sikring av personopplysninger mht. til konfidensialitet, integritet og tilgjengelighet som ivaretas i andre deler av styringssystemet, må NHN også ivareta personvern ved å sikre at verdien personopplysninger blir behandlet etter personopplysningslovens krav. Dette innebærer å oppfylle krav til ansvarlighet både som behandlingsansvarlig/dataansvarlig og som en profesjonell databehandler som kan støtte andre virksomheter i deres arbeid med ansvarlighet. I tillegg skal NHN kjenne og forvalte verdien personopplysninger på en slik måte at NHN og NHNs kunder faktisk kan følge personvernregelverket og dette styringssystemet, og kan vise etterlevelse av dem.

2. Målgruppe

Retningslinjene gjelder for alle *ansatte og innleide*. Gjennom avtale kan retningslinjene gjøres gjeldende for relevante tredjeparter.

3. Omfang

Denne retningslinjen omfatter strategiske føringer for personvern gjeldende for hele NHN når NHN behandler eller legger til rette for å behandle personopplysninger for sin egen del (som behandlingsansvarlig for personopplysninger eller dataansvarlig for helseopplysninger) eller som del av et utviklings- eller databehandleroppdrag for andre virksomheter (hvor NHN i det siste tilfellet vil være databehandler).

Alle skal krav er obligatoriske og må etterleves. Dersom et skal krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess

Alle bør krav er anbefalinger og må vurderes i hvert enkelt tilfelle. Det kreves ikke et godkjent avvik dersom et bør krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

4. Faglig innhold

4.1 Retningslinje for behandling av personopplysninger

Retningslinje	Beskrivelse
R15.1.1	Bruk av leverandører NHN skal bare bruke leverandører som sikrer og dokumenterer etterlevelse av personvernregelverket, også der det kan skje overføring av personopplysninger ut av EU/EØS. Det samme gjelder når NHN er leverandør. Leverandørens behandling av personopplysninger skal dokumenteres i en databehandleravtale.
R15.1.2	Rolleavklaring NHN skal avklare om NHN har rollen som behandlingsansvarlig/dataansvarlig eller databehandler ved behandling av personopplysninger og dokumentere dette.
R15.1.3	Personvernprinsipper NHN skal ivareta behandling av personopplysninger innenfor rammen av personvernprinsippene: • lovlighet • rettferdighet • åpenhet • formålsbestemthet • gjenbruksbegrensning • nødvendighet og forholdsmessighet • dataminimering • lagringsbegrensning • riktighet Prinsippene skal ivaretas i utvikling av nye løsninger, jf. Retningslinje for programvaresikkerhet og innebygd personvern. Det skal foreligge rutiner for å etterleve prinsippene.
R15.1.4	Personopplysningssikkerhet (konfidensialitet, integritet og tilgjengelighet) Personopplysninger skal behandles i henhold til NHNs styringssystem for sikkerhet og personvern slik at NHN sikrer tilstrekkelig vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade. Personopplysninger skal behandles slik at NHN sikrer at opplysningene er tilgjengelige for de som har tjenstlig behov for dem. Ved brudd på personopplysningssikkerheten skal Retningslinje for avviksbehandling følges.
R15.1.5	Rettigheter De registrertes rettigheter til informasjon, retting, sletting, retten til å bli glemt og til å motsette seg behandling skal ivaretas innenfor rammen av personvernregelverket og annen lovgivning.

	Det skal være enkelt og effektivt for en registrert å få innsyn i sine opplysninger som NHN er behandlingsansvarlig (dataansvarlig) for, og ellers forstå rettighetene og utøve dem.
R15.1.6	Personvernkonsekvenser All behandling av personopplysninger skal vurderes med tanke på hvilke konsekvenser behandlingen får for de registrerte og deres rettigheter og friheter. Vurderingen skal dokumenteres.
R15.1.7	Dokumentasjon NHN skal dokumentere etterlevelse av personvernregelverket i behandling av personopplysninger gjennom de verdikjedene NHN er en del av eller leverer. All behandling av personopplysninger skal vurderes før oppstart av behandling og dokumenteres i: • protokoll • risikovurdering • personvernkonsekvensvurdering (DPIA) • vurdering av overføring til ikke godkjente tredjeland, eller leverandører i USA som ikke er sertifisert i EU-US Data Privacy Framework • databehandleravtale • personvernerklæring Dokumentasjonen skal oppdateres eller vurderes oppdatert hver gang det skjer endringer i tjenesten som dokumentasjonen gjelder. NHN skal tilrettelegge dokumentasjon for innsyn for registrerte, kunder og tilsynsmyndigheter