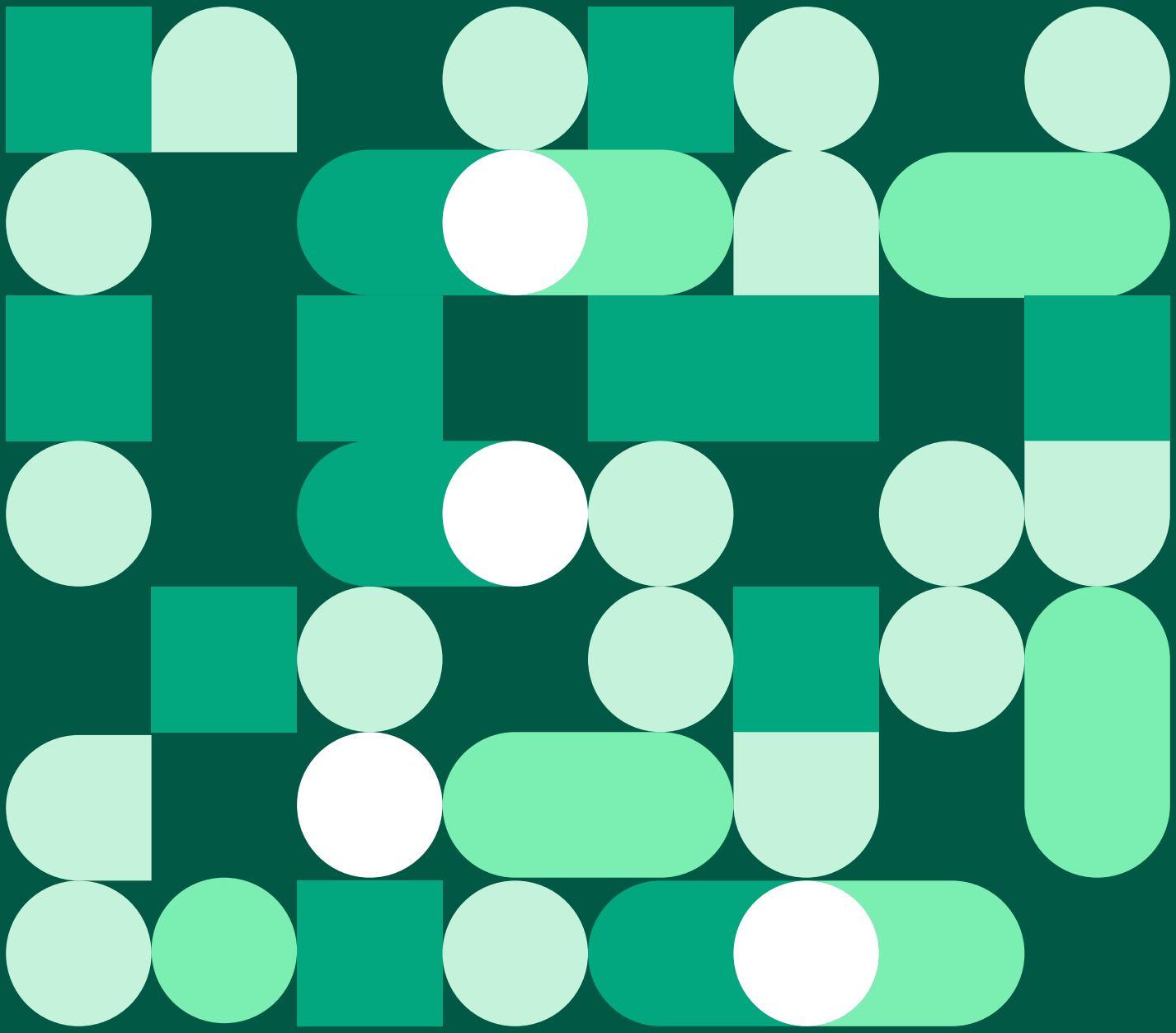

Retningslinjer for sikkerhet og personvern

Norsk helsenett

Innhold

01 Overordnet retningslinje for sikkerhet og personvern i NHN

Versjon 1.0

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 helsedata forvaltes i henhold til lovpålagte krav og befolkningens rett til vern av privatlivet, 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 og kravene i Normen.

02 Organisering av sikkerhets- og personvernarbeid

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. Hensikten med denne retningslinjen er å gi de overordnede føringene for organisering av sikkerhets- og personvernarbeidet i Norsk Helsenett (NHN), og sikre at sikkerhets- og personvernorganisasjonen understøtter NHNs strategiske føringer.

2. 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.

3. MÅLGRUPPE

Denne retningslinjen gjelder for alle *ansatte* og *innleide*. Gjennom avtale kan denne retningslinjen gjøres gjeldende for relevante tredjeparter.

4. KRAV

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 referanse.

Merk at 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.

Merk at 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.

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

4.1 Retningslinjer for organisering

Retningslinje	Beskrivelse
1	Organisering av sikkerhets- og personvernarbeidet i NHN SKAL være tydelig definert gjennom tydelige beskrivelser av roller/funksjoner og ansvar
2	Administrerende direktør i NHN SKAL ha det overordnede ansvaret for sikkerhet og personvern, og er eier av overordnet retningslinje for sikkerhet og personvern.
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. Seksjonen består av sikkerhetsdirektøren og sikkerhetsledere.
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.
5	Sikkerhetsleder SKAL lede, koordinere, kontrollere og veilede arbeidet innen ett eller flere fagområder i NHN, og jobber primært med styringsgrunnlag og retningslinjer.
6	NHN SKAL ha et personvernombud, som er virksomhetens uavhengige ressurs på personvernområdet. Personvernombudet SKAL lede og bidra i arbeidet med personvern og informere og gi råd om de forpliktelsene NHN har etter personvernlovgivningen til den behandlingsansvarlige eller databehandleren, samt til de ansatte som utfører behandlingen av personopplysninger. Personvernombudet SKAL være virksomhetens kontaktpunkt mot Datatilsynet, og rapporterer direkte til administrerende direktør i personvernrelaterte saker.
7	Funksjonen *NHN-SOC* SKAL jobbe aktiv med å forebygge, oppdage og håndtere sikkerhetshendelser internt i NHNs infrastruktur, tjenester og produkter.
8	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.
9	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).
10	Kryptosikkerhetsleder SKAL føre daglig tilsyn med at sikkerhetsbestemmelsene for *kryptotjenesten* blir fulgt.
11	Kryptoforvalter SKAL forvalte *kryptomateriell* hos NHN

4.2 Retningslinjer for organisering underlagt sikkerhetsloven

Retningslinje	Beskrivelse
1	Det SKAL utpekes en sikkerhetsleder og en stedfortredende sikkerhetsleder som har det faglige ansvaret knyttet til sikkerhetsloven.
2	Datasikkerhetsleder SKAL utnevnes i tilknytning til fysisk lokasjon Oslo.
3	Administrerende direktør har delegert autorisasjonsansvar til sikkerhetsleder og beredskapsdirektør.

03 Retningslinje for programvaresikkerhet og innebygd personvern

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. Hensikten med denne retningslinjen er å beskrive obligatoriske krav knyttet til programvaresikkerhet og innebygd personvern. Denne retningslinjen bidrar til å konkretisere krav som støtter under NHNs overordnede sikkerhetsmål.

2. 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.

2.1 Hva vurderes som programvareutvikling?

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.

3. MÅLGRUPPE

Denne retningslinjen gjelder for alle *ansatte* og *innleide*. Gjennom avtale kan denne retningslinjen gjøres gjeldende for relevante tredjeparter.

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

Retningslinjen tar utgangspunkt i Normen og NSM Grunnprinsipper, se referanse 1 og 2, og generell sikkerhetspraksis.

Merk at 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.

Merk at 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.

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

Retningslinje	Beskrivelse
1	NHN SKAL ha prosesser for sikker programvareutvikling slik at utviklingsprosessen bidrar til å ivareta innebygd sikkerhet og personvern. ▪ Sikkerhetsarbeidet skal være forankret i risikostyring
2	Det SKAL være etablert og vedlikeholdt en helhetlig sikkerhetsarkitektur som ivaretar et sikkert og motstandsdyktig IKT-system.
3	Det SKAL bygges produkter som samhandler godt sammen sikkerhets- og personvernmessig.
4	Det SKAL være tilstrekkelig separasjon mellom utvikling, test, QA/Akseptanse test og produksjon. Operative virksomhetsprosesser skal ikke bli påvirket av feil i utviklings- og testmiljøer.
5	NHN SKAL sikre at data som benyttes til utviklings- og testformål ikke inneholder *personopplysninger*.
6	NHNs utviklingsprosesser SKAL ta særskilt høyde for å ivareta krav til sikkerhet i løsninger der informasjon om personer med skjermet adresse (Fortrolig og strengt fortrolig) utvikles, etter retningslinjer i Normen v6.0 faktaark 55.
7	Det SKAL utføres tilstrekkelig med sikkerhetstesting som en integrert del av utviklingsprosessen.
8	Ved bruk av offentlig tilgjengelig kode (*«open source»*) og kommersielle *«toolkits»* SKAL det regelmessig, og fortrinnsvis automatisk, sjekkes for sårbarheter og kontrollert oppdateres til nye versjoner.

4.2 Retningslinje for programvaresikkerhet og innebygd personvern i prosjekter

Retningslinje	Beskrivelse
1	Retningslinje i avsnitt 4.1 gjelder også for prosjekter
2	Prosjektmodellen i NHN SKAL spesifisere dedikert budsjettering for finansielle midler til gjennomføring av sikkerhets- og personvernaktiviteter gjennom prosjektets livssyklus.
3	Arbeid med sikkerhet og personvern SKAL være tydelig beskrevet i prosjektmetodikken. Dette arbeidet SKAL etterleve retningslinje i avsnitt 4.1 og Standard for programvaresikkerhet og innebygd personvern.

04 Retningslinje for risikostyring av informasjonssikkerhet

Versjon 1.1

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. Hensikten med denne retningslinjen er å beskrive obligatoriske krav for risikostyring av informasjonssikkerhet og personvern i virksomheten.

2. 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.

3. MÅLGRUPPE

Denne retningslinjen gjelder for alle *ansatte* og *innleide*. Gjennom avtale kan denne retningslinjen gjøres gjeldende for relevante tredjeparter.

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.

Merk at 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.

Merk at 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.

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

4.1 Retningslinje for risikostyring

Retningslinje	Beskrivelse
1	NHN SKAL fastsette nivå for akseptabel risiko i virksomhetens informasjonssystemer gjennom akseptkriterier.
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.
3	Alle tjenester, registre og informasjonssystemer SKAL ha en definert risikoeier.
4	Risikoeier SKAL sørge for at risiko rapporteres regelmessig til virksomhetens ledelse.
5	Risikostyring og risikonivå SKAL dokumenteres. Dokumentasjon inkluderer risikovurderinger, eierskap, sporbare beslutninger, sikkehetsavvik og plan for å oppnå akseptabel risiko.
6	NHNs ledelse SKAL jevnlig følge opp virksomhetens risikonivå med formål å drive forsvarlig virksomhetsstyring.

05 Retningslinje for aktiva og klassifisering

Versjon 1.1

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. Hensikten med denne retningslinjen er å stille krav som bidrar til at NHN har dokumentasjon på informasjon og utstyr. NHN skal forsikre seg om at informasjon behandles på en betryggende måte som ivaretar krav til sikkerhet og personvern.

2. 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.

3. MÅLGRUPPE

Denne retningslinjen gjelder for *alle ansatte og innleide*. Gjennom avtale kan denne retningslinjen gjøres gjeldende for relevante tredjeparter.

4. 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.

Merk at 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.

Merk at 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.

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

4.1 Retningslinje for aktiva

Retningslinje	Beskrivelse
1	NHN SKAL føre en oversikt over tjenester og tilhørende informasjonssystemer. Oversikten SKAL beskrive tjenestekritikalitet, eierskap og informasjonstyper for alle informasjonssystemer.
2	NHN SKAL føre et register over alle hardware og software komponenter som utgjør tjenester i drift. Registeret SKAL beskrive status og komponentenes relasjon og avhengighet til hverandre.
3	Det SKAL føres protokoll over *behandling* av *personopplysninger* i NHNs tjenester og informasjonssystemer, både når NHN er *behandlingsansvarlig* og *databehandler*. Innholdet i protokollen SKAL være i samsvar med *personvernforordningen* artikkel 30.

4.2 Retningslinje for aktiva underlagt sikkerhetsloven

Retningslinje	Beskrivelse
1	Det SKAL føres oversikt over hvilke dokumenter som oppbevares hos NHN, og som i henhold til sikkerhetsloven er sikkerhetsgradert.
2	Sikkerhetsnivået for NHNs arkivsystem og oppbevaringsløsninger for sikkerhetsgradert informasjon SKAL være tilpasset sikkerhetsgrad **KONFIDENSIELT**.
3	Informasjon som er gradert høyere enn **KONFIDENSIELT** SKAL IKKE behandles i virksomheten.
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*.
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
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.
2	Informasjonstyper og tilhørende *sikkerhetsklasser* SKAL være beskrevet og gjort tilgjengelig som hjelpemiddel for alle ansatte og innleide.
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 1.1

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. Hensikten med denne retningslinjen er å beskrive obligatoriske krav knyttet til drift og forvaltning.

2. 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

3. MÅLGRUPPE

Denne retningslinjen gjelder for *alle ansatte og innleide*. Gjennom avtale kan denne retningslinjen gjøres gjeldende for relevante tredjeparter.

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*.

Merk at alle SKAL-krav er obligatoriske og må etterleves. Dersom et SKAL-krav ikke kan etterleves, må det registreres som et avvik i henhold til NHN sin avviksprosess.

Merk at alle BØR-krav er veiledende og kan vurderes i hvert enkelt tilfelle. Det kreves ikke et registrert avvik dersom et BØR-krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

4.1 Retningslinje for sikkerhet i operasjonell drift

Retningslinje	Beskrivelse
1	NHN SKAL sikre at informasjon og systemer har tilstrekkelig sikkerhet for å ivareta integritet, konfidensialitet og tilgjengelighet i henhold til vedtatt risikoaksept.
2	NHN SKAL sørge for at informasjon og informasjonssystemer er beskyttet mot skadevare og ondsinnede angrep.
3	NHN SKAL gjennom rutiner og definert ansvar for informasjonssystemer sikre at systemer til enhver tid er oppdatert og oppgradert.
4	NHN SKAL sørge for at alt utstyr, tjenester og programvare logger i henhold til loggkrav fastsatt i egen standard.
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.
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.
7	NHN SKAL ha systemer for å identifisere og detektere sårbarheter i teknisk infrastruktur.
8	NHN SKAL sikre at det ikke ligger igjen virksomhetskritisk informasjon eller personopplysninger som kan komme på avveie ved avhending av utstyr.
9	NHN SKAL dokumentere hvordan sikkerhet og personvern sikres i tjenestene gjennom å beskrive hvordan konfidensialitet, integritet og tilgjengelighet ivaretas.
10	NHN SKAL gjennomføre inntrengningstester mot egne tjenester og infrastruktur ved større endringer, og eller minimum en gang per år.
11	NHN SKAL håndtere endringer knyttet til operasjonell drift gjennom en etablert endringsprosess.

07 Retningslinje for fysisk sikkerhet

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. Hensikten med denne retningslinjen er å beskrive obligatoriske krav knyttet til fysisk sikkerhet.

2. 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

3. MÅLGRUPPE

Denne retningslinjen er obligatorisk og omfatter alle faste og midlertidig ansatte, vikarer og innleide. Gjennom avtale kan denne retningslinjen gjøres gjeldende for *relevante tredjeparter*.

4. FAGLIG INNHOLD

Retningslinje	Beskrivelse
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.
2	Tilgang til NHNs fysiske lokaler SKAL kun gis til personell med tjenstlig behov, og tilgang til fasiliteter med særlig skjermingsbehov (f.eks. datasentre) SKAL logges.
3	NHN SKAL ha etablerte rutiner og tiltak som hindrer uautorisert tilgang til ubevoktet utstyr.

Retningslinje	Beskrivelse
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
5	NHN SKAL gjøre en vurdering av redundans eller alternative lokaler for drift der tjenester som i henhold til kritikalitet krever høy oppetid.
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.
7	NHN SKAL etablere løsninger som sikrer mot uautorisert tilgang til data hvis mobilt utstyr eller bærbare medier havner på avveie.
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.
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.
10	Adgangskort med bilde SKAL bæres synlig så lenge man oppholder seg i NHNs fysiske lokaler.

08 Retningslinje for avviksbehandling

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. Hensikten med denne retningslinjen er å beskrive obligatoriske krav knyttet til virksomhetens behandling av avvik.

2. OMFANG

Retningslinjen dekker kravene til avvikssystem og prosess for avvikshåndtering.

3. MÅLGRUPPE

Denne retningslinjen er obligatorisk og omfatter alle faste og midlertidig ansatte, vikarer og innleide. Gjennom avtale kan denne retningslinjen gjøres gjeldende for relevante tredjeparter.

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.

Merk at alle SKAL-krav er obligatoriske og må etterleves. Dersom et SKAL-krav ikke kan etterleves, må det registreres som et avvik i henhold til NHN sin avviksprosess.

Merk at alle BØR-krav er veiledende og kan vurderes i hvert enkelt tilfelle. Det kreves ikke et registrert avvik dersom et BØR-krav ikke implementeres, men det anbefales at avgjørelsen baseres på en risikovurdering.

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

Retningslinje	Beskrivelse
1	NHN SKAL ha et avvikssystem og tilhørende rutiner for oppfølging av avvik.
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.
3	Alle ansatte, innleide og *relevante tredjeparter* SKAL innrapportere umiddelbart når de oppdager eller har mistanke om et avvik.
4	Avvik SKAL følges opp i hver enkelt divisjon, og divisjonsdirektør har det overordnede ansvaret for avviksoppfølging i egen divisjon.
5	Personvernombudet SKAL informeres umiddelbart ved mistanke om brudd på *personopplysningssikkerheten*.
6	Personvernombudet SKAL vurdere om avviket utgjør et brudd på personopplysningsikkerheten. Dersom Norsk helsenett er dataansvarlig SKAL slike brudd meldes til Datatilsynet innen 72 timer.
7	Linjeleder SKAL etablere en tiltaksplan for å lukke innmeldte avvik, og med en prioritering som hensyntar avvikets kritikalitet.
8	Sikkerhetsavvik 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 1.2

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. Hensikten med denne retningslinjen er å legge føringer for avtaleverk mellom arbeidsgiver og arbeidstaker, og ansvaret som ligger på HR funksjonen og ledere for å sikre personellsikkerhet.

2. 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.

3. MÅLGRUPPE

Denne retningslinjen er obligatorisk og omfatter alle faste og midlertidig ansatte, vikarer og innleide. Målgruppe er spesielt HR funksjonen og ledere med personalansvar. Gjennom avtale kan denne retningslinjen gjøres gjeldende for *relevante tredjeparter*.

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.

Merk at 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.

Merk at 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.

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

Retningslinje	Beskrivelse
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.
2	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.
3	Ansatte og innleid personell, inkludert personell hos underleverandører, som skal jobbe med *skjermingsverdige objekter* eller *infrastruktur*, som definert i Sikkerhetsloven, SKAL kunne sikkerhetsklareres eller adgangsklareres på tilstrekkelig nivå.
4	Ansatte eller innleid personell, inkludert personell hos underleverandører, som skal jobbe med *tjenester underlagt sikkerhetsloven* SKAL inneha tilstrekkelig sikkerhetsklarering og autorisasjon i henhold til kravene i Sikkerhetsloven.
5	Retningslinje for bruk av kontor, hjemmekontor og fjernarbeid SKAL følges.
6	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*.
7	Innleide SKAL signere og akseptere *taushetserklæring* og *sikkerhetsinstruks* før det gis tilgang til NHNs informasjon eller informasjonssystemer. Dokumentene SKAL arkiveres i NHN sitt *arkivsystem*.
8	Personer uten arbeidsavtale som gis midlertidig tilgang til NHNs informasjon og informasjonssystemer, SKAL signere taushetserklæring før tilgang til informasjonen gis. Behov for signering av sikkerhetsinstruks skal vurderes av linjeleder i det enkelte tilfelle.
9	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.
10	Linjeledere SKAL sørge for at ansattes og innleides tilganger blir tilbaketrukket ved endring eller opphør av *ansettelsesforhold* eller *innleieperiode*.

10 Retningslinje for sikkerhet og personvern i anskaffelser og kontraktsoppfølging

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. Hensikt med denne retningslinjen er å gi de overordnede krav og føringer for ivaretakelsen av informasjonssikkerhet og personvern i anskaffelsesprosessen, herunder kontraktsoppfølging i NHN. Formålet med dokumentet er å etablere en strukturert tilnærming, enhetlig begrepsbruk og felles forståelse for krav til informasjonssikkerhet og personvern i anskaffelser og kontraktsoppfølging, og tydeliggjøre ansvarsområder.

2. 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.

3. MÅLGRUPPE

Denne retningslinjen gjelder for alle *ansatte* og *innleide*. Gjennom avtale kan denne retningslinjen gjøres gjeldende for *relevante tredjeparter*.

4. FAGLIG INNHOLD

Følgende forhold skal ivaretas i arbeidet med offentlige anskaffelser i NHN, for å sikre tilstrekkelig ivaretakelse av behov knyttet til informasjonssikkerhet og personvern i h.h.t. underliggende kontrakt. For nærmere beskrivelse se i standard for anskaffelser og kontraktsoppfølging.

Merk at 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.

Merk at alle BØR-krav er veiledende og kan 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.

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

Retningslinje	Beskrivelse
1	NHN SKAL etablere og vedlikeholde oversikt over alle avtaler og leverandører.
2	NHN er underlagt lov om offentlig anskaffelser. Krav til informasjonssikkerhet og personvern SKAL bli tatt inn som del av konkurransegrunnlaget.
3	NHN SKAL ha prosesser som sikrer at krav til informasjonssikkerhet og personvern i leverandørforhold og anskaffelser ivaretas i hele livsløpet fra planlegging, leveranse og oppfølgingsfasen til avslutning av leverandørforholdet.
4	Krav til informasjonssikkerhet og personvern SKAL ivareta den tekniske utviklingen og trusselbildet over tid.
5	Krav til informasjonssikkerhet og personvern SKAL tilpasses det som skal anskaffes med utgangspunkt i en risikovurdering
6	NHN SKAL ha oversikt over hele leverandørkjeden, inkludert underleverandører av NHNs leverandører. Det må sikres at krav til informasjonssikkerhet og personvern også gjenspeiles videre i leverandørkjeden.
7	Informasjonssikkerhet og personvern SKAL også ivaretas ved avslutning av leverandørforholdet i h.h.t. kontrakt. ▪ Det SKAL sikres at leverandøren ved avslutning av leverandørforholdet tilbakefører NHNs informasjon. ▪ Leverandøren SKAL bekrefte og dokumentere at NHNs informasjon er slettet hos leverandøren og alle underleverandører samt at alle tilganger er stengt.
8	Det SKAL vurderes om det er behov for å gjennomføre en personvernkonsekvensvurdering (DPIA) av produktet/tjenesten, dersom produktet/tjenesten vil medføre en behandling av personopplysninger.
9	Dersom det vil behandles personopplysninger SKAL relevante personvernforhold dokumenteres.

Retningslinje	Beskrivelse
10	Leverandører vil ofte kunne være å anse som en databehandler/*underdatabehandler*. I utgangspunktet SKAL NHN sin mal for databehandleravtaler benyttes for NHN sine egne anskaffelser. Unntaksvis kan leverandørens databehandleravtale eller eventuelt standardvilkår aksepteres, dersom juridisk avdeling vurderer at standardvilkårene tilstrekkelig ivaretar regulatoriske krav og kravene til informasjonssikkerhet og personvern i NHN sin databehandleravtale.
11	Hver divisjon har et selvstendig ansvar for å følge opp at leverandørene de benytter ivaretar informasjonssikkerhet og personvern slik det fremkommer av avtalen.
12	Divisjon Sikkerhet har ansvar for at det regelmessig foretas ettersyn/revisjoner av et utvalg av leverandøravtalene med henblikk på krav til informasjonssikkerhet og personvern.

11 Retningslinje for kryptografi

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. Krypteringsløsninger er helt sentrale i arbeidet med digital sikkerhet, og denne retningslinjen bidrar til å:

- Legge til rette for sikkerhet og effektiv digital samhandling i helse- og omsorgstjenesten.
- Ivareta sikker og stabil drift av kritiske IKT-tjenester.
- Sikre at helsedata forvaltes i henhold til lovpålagte krav og befolkningens rett til vern av privatlivet.

2. 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.

3. MÅLGRUPPE

Denne retningslinjen gjelder for alle *ansatte* og *innleide*. Gjennom avtale kan denne retningslinjen gjøres gjeldende for *relevante tredjeparter*.

4. FAGLIG INNHOLD

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

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

Retningslinje	Beskrivelse
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.
2	*Kryptomateriell* SKAL kun forvaltes av *autorisert personell*, og lagres på tilstrekkelig sikrede og tilgangskontrollerte områder.

Retningslinje	Beskrivelse
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.
4	Alle trådløse nettverksforbindelser i, og levert av, Norsk helsenett skal krypteres.
5	Kryptering av *lagrede data* skal vurderes som et sikringstiltak og behovet skal vurderes i en risikovurdering.
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.
7	Kryptering skal følge oppdaterte, anerkjente og robuste standarder, basert anbefalinger fra Nasjonal Sikkerhetsmyndighet (NSM Cryptographic Requirements) og være motstandsdyktige mot aktive og passive angrep.
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).
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.
10	Kryptoalgoritmer og nøkler SKAL kunne byttes ut, for eksempel dersom algoritme eller nøkler blir kompromittert.
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 1.1

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.

Norsk Helsenett skal sørge for at alle *informasjonssystemer*, lagringsområder og tilhørende informasjon er sikret med tilstrekkelig tilgangsstyring. Retningslinjen har som hensikt å legge føringer som sikrer at riktige personer får riktige tilganger, til riktig tid, og av riktig grunn.

2. 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.

3. MÅLGRUPPE

Denne retningslinjen gjelder for alle *ansatte* og *innleide*. Gjennom avtale kan denne retningslinjen gjøres gjeldende for *relevante tredjeparter*.

4. FAGLIG INNHOLD

Retningslinjen setter krav til brukeradministrasjon og tilgangskontroll for alle informasjonssystemer NHN forvalter. Kravene gjelder for de som administrerer brukertilganger i NHN, og det er krav som gjelder for alle som har fått en bruker i NHN. Krav i denne retningslinjen er også gjeldende for eksterne leverandører og for utkontraktert utvikling.

Merk at 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.

Merk at alle BØR-krav er veiledende og kan 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.

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

4.1 Retningslinje for brukeradministrasjon

Retningslinje	Beskrivelse
1	NHN SKAL ha dokumenterte prosesser for brukeradministrasjon. Dette inkluderer dokumenterte prosesser for å opprette, endre, deaktivere og slette brukerkontoer.
2	Alle personlige brukerkontoer i NHN SKAL knyttes til en bestemt person.
3	Alle *ikke-personlige kontoer* SKAL være unike, og kontoene skal være knyttet til en bestemt enhet.
4	Alle brukere i NHN SKAL ha unike kombinasjoner av brukernavn og passord.
5	Det SKAL foreligge en dokumentert og sikker prosess for formidling av brukernavn og passord.
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.
7	NHN SKAL ha oversikt over hvilke brukere som har tilgang til informasjonssystemer, og hvilke tilgangsrettigheter de har.
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.
9	Brukere og brukernes tilganger SKAL revideres minimum en gang per år, med særlig fokus på privilegerte tilganger. Revisjonen SKAL sikre at tilganger til ansatte og innleid personell er trukket tilbake når arbeidsforhold eller kontraktsforhold har opphørt, og at tilganger følger tjenstlig behov. Revisjonen skal dokumenteres.

4.2 Retningslinje for tilgangskontroll

Retningslinje	Beskrivelse
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.
2	Alle tilganger til informasjonssystemer SKAL baseres på tjenstlig behov.

Retningslinje	Beskrivelse
3	Informasjonssystemer BØR integreres med sentral katalogtjeneste for å forenkle bruke-radministrasjonen, og sikre at tilganger til alle informasjonssystemer kan kontrolleres, og ved behov sperres, fra sentral kilde.
4	Det SKAL eksistere tydelige retningslinjer for krav til passord, passordhvelv, engangsko-der, og hvordan de skal håndteres.
5	All tilgang til informasjonssystemer som inneholder informasjon klassifisert som intern/ virksomhetskritisk, og som er publisert på internett SKAL være beskyttet med multi-fak-tor autentisering.

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

Retningslinje	Beskrivelse
1	Som hovedregel SKAL NHNs retningslinje for brukeradministrasjon og tilgangskontroll følges, med mindre kunden har instruert NHN om annen praksis.
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 informasjons-systemer. Denne informasjonen skal kunne oversendes kunde på forespørsel.
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 tilgangs-rettigheter 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 tilgan-ger til kundens informasjonssystemer.

13 Retningslinje for beredskap og kontinuitetsplanlegging

Versjon 1.1

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.

Denne retningslinjen bidrar til å gi føringer og beskrive obligatoriske krav for beredskap og kontinuitetsplanlegging i NHN.

2. OMFANG

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

3. MÅLGRUPPE

Denne retningslinjen gjelder for alle *ansatte* og *innleide*. Gjennom avtale kan denne retningslinjen gjøres gjeldende for relevante tredjeparter.

4. RETNINGSLINJE FOR BEREDSKAP OG KONTINUITETSPLANLEGGING

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.

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

Retningslinje	Beskrivelse
1	NHN SKAL vurdere konsekvensene av et avbrudd for virksomheten, også kjent som BIA (business impact analysis). Konsekvensvurderingen skal omfatte både en overordnet vurdering og en konsekvensvurdering av produkter og tjenester. ▪ Konsekvensvurderingen skal identifisere behov for å etablere alternativ driftsløsning og redundans som sikrer kontinuitet ved uforutsett driftsstans.
2	NHN SKAL etablere *kontinuitetsplan* og *gjenopprettingsplan* for håndtering av *major incidents* tilknyttet produkter og tjenester som ledelsen har definert som høy og kritisk (i henhold til standard for klassifisering og tjenestekritikalitet).
3	NHN SKAL etablere *beredskapsplanverk* for håndtering av kriser. Beredskapsplanverket skal definere roller og ansvar og gi krav for organisering i en *krise*.
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.

14 Retningslinje for samsvar og internkontroll

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. NHN knytter helsetjenesten sammen og gjør helsedata og IKT-tjenester tilgjengelig for helseforvaltningen, helsepersonell, pasienter og befolkningen forøvrig.

Hensikten med denne retningslinjen er å gi de overordnede føringene for NHNs arbeid med å forebygge og avdekke avvik fra krav i styringssystemet for informasjonssikkerhet.

2. 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.

3. MÅLGRUPPE

Denne retningslinjen gjelder for alle *ansatte* og *innleide*. Gjennom avtale kan denne retningslinjen gjøres gjeldende for *relevante tredjeparter*.

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.

Merk at 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, se referanser.

Merk at alle BØR-krav er veiledende og kan 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. .

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

4.3 Retningslinje for samsvar og internkontroll

Retningslinje	Beskrivelse
1	NHN skal sikre at tjenesteleveransene og forvaltningen av data til enhver tid er i samsvar med gjeldende lovverk.
2	NHN skal sikre at tjenesteleveransene og forvaltningen av data til enhver tid ivaretar sikkerhets- og personvernskrav vi har forpliktet oss til gjennom etablerte kontrakter.
3	Hver divisjon har et selvstendig ansvar for å sikre etterlevelse av lovpålagte krav, kundeforpliktede sikkerhets- og personvernkrav (for eksempel inngåtte databehandleravtaler) og kravene i styringssystemet for sikkerhet og personvern innenfor eget ansvarsområde.
4	Sikkerhetsdivisjonen skal etablere et årshjul for revisjon som sikrer en systematisk og planlagt gjennomføring av revisjons- og internkontrollarbeid, med formål å oppdage avvik fra etablerte retningslinjer i styringssystemet.

15 Retningslinje for behandling av personopplysninger

Versjon 1.0

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. 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).

3. MÅLGRUPPE

Denne retningslinjen er obligatorisk og omfatter alle faste og midlertidig ansatte, vikarer og innleide.

4. KRAV TIL BEHANDLING AV PERSONOPPLYSNINGER

Merk at alle SKAL-krav er obligatoriske og må etterleves før oppstart av behandling av personopplysningene. Dersom et SKAL krav ikke kan etterleves, må det registreres og godkjennes som et avvik i henhold til NHN sin avviksprosess, se referanser.

Merk at alle BØR-krav er veiledende og kan 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.

Merk at alle begreper i *kursiv* er definert i den begrepslisten som ligger nederst i dokumentet.

Retningslinje	Beskrivelse
1	**Etterlevelse** NHN SKAL sikre og SKAL dokumentere etterlevelse av personvernregelverket i behandling av personopplysninger gjennom de verdikjedene NHN er en del av eller leverer.
2	**Bruk av leverandører** NHN SKAL sikre at NHN bare bruker leverandører som sikrer og dokumenterer etterlevelse av personvernregelverket, og behandlingen SKAL dokumenteres i en databehandleravtale.
3	**Rolleavklaring** NHN SKAL avklare om NHN har rollen som behandlingsansvarlig/dataansvarlig eller databehandler ved behandling av personopplysninger og dokumentere dette.
4	**Personvernprinsipper** NHN SKAL vurdere all behandling av personopplysninger med hensyn til ▪ 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.

Retningslinje	Beskrivelse
5	**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.
6	**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 forstå rettighetene og utøve dem.
7	**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.
8	**Dokumentasjon** All behandling av personopplysninger SKAL dokumenteres i protokoll, og gjenbrukes for ▪ risikovurdering ▪ personvernkonsekvensvurdering (DPIA) ▪ vurderinger av overføring til ikke godkjente tredjeland (”Schrems”) ▪ 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.

16 Begrepsliste

Begrep	Beskrivelse
A eller B feil	Major incident; Høyeste kategorier tildelt en IKT-hendelse for dens påvirkning. Major incident regnes som innenfor ”normale driftsrutiner”.
Aktiva	Alt som er av verdi for Norsk Helsenett. Aktiva kan være programvare, maskinvare, fysiske lokaler, datarom, personell, dokumenter, informasjon og informasjonssystemer.
Adgangsklarert personell	Personell som skal ha fysisk adgang til en tjeneste eller et objekt som er definert som skjermingsverdig må adgangsklareres av Sivil klareringsmyndighet iht kravene i Sikkerhetsloven.
Aktivaregister	Et sentralt register over tjenesteområder og tilhørende informasjonssystemer.
Ansatte	Alle faste og midlertidig ansatte (tidligere er medarbeider benyttet som begrep). En midlertidig ansatt kan være en vikar, sommerstudenter o.l.
Ansettelsesforhold	Et arbeidsforhold mellom en ansatt (faste eller midlertidig ansatte) og Norsk Helsenett som arbeidsgiver.
Arbeidsforhold	Et avtaleforhold hvor en ansatt eller innleid forplikter seg til å utføre arbeid for Norsk Helsenett. Begrepet omfatter både ansettelsesforhold og oppdragsforhold.
Arkivsystem	System som benyttes til å registrere, administrere, oppbevare og gjenfinne dokumentene som inngår i et arkiv.
Autorisert personell (ift. sikkerhetsgradert informasjon)	Ansatt eller innleid som er autorisert til å behandle sikkerhetsgradert informasjon. Informasjon som er over grad BEGRENSET trenger i tillegg Sikkerhetsklarering.
Avtaleforhold	Et avtaleforhold hvor en ansatt eller innleid forplikter seg til å utføre arbeid for Norsk Helsenett. Begrepet omfatter både ansettelsesforhold og oppdragsforhold.

Begrep	Beskrivelse
Avvik	Et avvik er en uønsket hendelse eller en mulig uønsket hendelse, og kan ha ulik kritikalitet. Eksempler på avvik ▪ Brudd på gjeldende rutiner eller regelverk (styringssystemer eller lovpålagte krav) ▪ 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.
Behandling (av personopplysninger)	Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring, jf. personvernforordningen (GDPR) artikkel 4 nr. 2.
Behandlingsansvarlig (dataansvarlig)	En fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett, jf. personvernforordningen (GDPR) artikkel 4 nr. 7.
Behandlingsprotokoll	En protokoll eller oversikt over alle behandlinger av personopplysninger som utføres av en virksomhet.
Beredskapsplanverk	Kriser utløser beredskapsplanverket. Beredskapsplanverket beskriver hvordan alle typer kriser skal håndteres, inkludert kriser som ikke direkte berører IKT. Eksempler på slike kriser er brann eller annen større ulykke i NHN sine lokaler, ulykke der ansatte på tjenestereise er involvert eller bombetrussel/ terror rettet mot NHN eller NHN sine ansvarsområder.
BIA	Business Impact Analysis - forretningskonsekvensvurdering/ virksomhetskonsekvensvurdering/konsekvensvurdering.
BYOD	Bring Your Own Device. Privat utstyr eller utstyr administrert av en annen virksomhet enn NHN.
C eller D hendelser	Hendelse, Incident: Et ikke-planlagt avbrudd i en IT-tjeneste, eller en reduksjon i kvaliteten til en IT-tjeneste.
CMDB	Configuration management database, utstyrsdatabase.

Begrep	Beskrivelse
Databehandler	En fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. personvernforordningen (GDPR) artikkel 4 nr. 8.
Disiplinær prosess	Ved en ansatts eller innleids brudd på krav i styringssystemet, skal leder vurdere om det skal iverksettes en reaksjon mot den ansatte eller innleide. Leder har ansvar for at sikkerhetsbruddet verifiseres. Reaksjonen skal vurderes opp mot sikkerhetsbruddets alvorlighet.
Dokument	Informasjon som er lagret på et medium for senere lesing, lytting, fremføring, overføring eller lignende.
DPIA	Vurdering av personvernkonsekvenser i henhold til personvernforordningen (GDPR) artikkel 35 (*Data Protection Impact Assessment*).
Driftsrapport	Månedlig driftsrapport for hver tjeneste som skal leveres i Driftsspacet i Confluence
Driftsspace	Den enkelte tjenestes område i Confluence
Driftsteam	Team som har ansvar for drift av en løsning/løsninger, hvor tjenesteansvarlig og driftsansvarlig har utvidet ansvar.
Endepunkstutstyr	F.eks servere, klienter, API'er, eller komponenter som eksponerer API'er
EOS	End of support, Dato som leverandør setter for når de slutter å supportere en versjon/produkt.
EOL	End of life, Dato som leverandør setter for slutt av videreutvikling/patching av en versjon/produkt.
Gjenopprettingsplan	Gjenopprettingsplaner SKAL ivareta at produktområdene gjenopprettes til akseptabelt nivå innenfor fastsatt tidsramme etter et brudd.
HCL	Hardware Compability List – oversikt over kombinasjoner av HW og SW som er supportert.
HelseCERT	Helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet. HelseCERTs oppgave er å øke sektorens evne til å oppdage, forebygge og håndtere ondsinnede inntrengingsforsøk og andre uønskede IKT-hendelser. HelseCERT skal spre kunnskap om IKT-trusler og beskyttelsesmekanismer og kontinuerlig monitorere trafikken i Helsenettet. HelseCERT er en seksjon i Norsk Helsenett og er lokalisert i Trondheim.

Begrep	Beskrivelse
Helsenettet	Helsenettet er en lukket og sikret kommunikasjonsarena som består av alle tilknyttede virksomheter, de tjenestene de benytter, samt de kommunikasjonselementene og –systemene som binder dem sammen og muliggjør utveksling av personopplysninger innenfor rammen av Normen.
HW	Hardware (Servere, lagring, nettverksutstyr osv)
Informasjon	Ett eller flere informasjonselementer eller ulike typer (digitale eller fysiske) dokumenter.
Innleid	En person ansatt hos en leverandør som er leid inn av NHN til å utføre arbeidsoppgaver i henhold til anskaffelse/kontrakt
Informasjonssystem	System eller register med tilhørende teknisk infrastruktur.
Informasjonstype	Forhåndsklassifisert kategori av informasjon, for eksempel personopplysninger, helseopplysninger, system- og driftsdokumentasjon, fødselsnummer, regnskap, eller rapporter.
Internkontroll	Systematiske tiltak som sikrer at virksomheten planlegger, organiserer, gjennomfører og opprettholder sine aktiviteter i samsvar med gjeldende krav i lover, forskrifter og regelverk.
Internrevisjon	Intern gjennomgang som er uavhengig, objektiv bekreftelses- og rådgivningsfunksjon med hensikt å tilføre merverdi og forbedre organisasjonens drift.
Klassesikring	Angir sikkerhetstiltak i henhold til informasjonssystemets sikkerhetsklasse.
Klassifisering	Angir hvilken klasse informasjon eller informasjonssystem er definert som (åpen, intern, skjermet, sterkt skjermet).
Klient	Maskinvare eller programvare som en bruker benytter for å kommunisere med en tjeneste på en en tjener/server
Kontinuitetsplan	Kontinuitetsplanverket sier noe om hvordan kontinuitet av et produkt eller tjeneste skal ivaretas ved en alvorlig IKT-hendelse . Kontinuitet har hovedfokus på å sikre tilgjengeligheten av informasjon og informasjonssystemer, og skal også ta hensyn til at informasjon ikke kommer på avveie (konfidensialitet) eller blir utsatt for uautoriserte endringer (integritet) slik at informasjonssikkerhetskontinuitet er ivaretatt.

Begrep	Beskrivelse
Kunde	Inkluderer hele den offentlige og private helse- og omsorgstjenesten, som gjennom medlemskap i Helsenettet bruker den sikrede infrastrukturen som Helsenettet innebærer. Inkluderer også virksomheter i Helseforvaltningen som kjøper IKT-, anskaffelses- og arkivtjenester av NHN.
Krise	En krise kjennetegnes ved at det er en situasjon som stiller så høye krav at organisasjonens normale rutiner og ressurser ikke strekker til.
Kryptomateriell	Alt som håndtere kryptografi, f.eks nøkler, sertifikater, kryptobokser/HSM moduler, tilgang til programvarebaserte hvelv, signeringstjenesten, virksomhetssertifikater osv.
Lagrede data	Data lagret på ulike formater, f.eks database, filstruktur, på disk osv.
Ledelse/Øverste ledelse	Organisasjonens leder har normalt det øverste ansvaret i en organisasjon. Øverste ledelse betegnes som den styrende delen av lederens arbeid. Som regel inkluderer dette lederens ledergrupper som også betegnes som "toppledergruppen".
Major incident	Alvorlig hendelse; A eller B hendelser, som håndteres gjennom et dedikert kontinuitetsplanverket.
MASL	Minimum Acceptable Service Level; Minimum akseptabelt servicenivå; handler om hvilke krav som stilles til oppetid totalt i løpet av en mnd. Forskjellen på MASL og MTPD/RTO, er at MTPD/RTO ser på kritisk tidsperiode for nedetid per gang, mens MASL ser på totalt krevd oppetid i løpet av en mnd.
MTPD	Maximum Tolerable Period of Disruption; Maksimalt akseptert nedetid; den maksimalt tillatte tiden organisasjonens nøkkelprodukter eller -tjenester blir gjort utilgjengelige eller ikke kan leveres før innvirkning anses som uakseptabel. MTPD gir det maksimale kritiske punktet for hver prosess eller ressurs/produkt.
Mindre hendelser	Mindre hendelser er C eller D hendelser, og håndteres gjennom normale rutiner og prosesser og krever ikke et eget dedikert planverk for håndtering.
NHN-SOC	NHNs funksjon for intern sikkerhetsovervåking (NHN-SOC)

Begrep	Beskrivelse
Noderom	Datarom benyttet til kommunikasjonsutstyr for blant annet stamnettet.
Normen	Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren. (www.normen.no)
Objekter eller infrastruktur	Eiendom og anlegg og systemer som må beskyttes mot tilsiktede uønskede hendelser av hensyn til opprettholdelse av grunnleggende nasjonale funksjoner.
OLA	Intern driftsavtale mellom interne driftsteam for å underbygge en tjenesteleveranse.
Open Source	Åpen kildekode (oftest omtalt med lånebegrepet open source fra engelsk) betyr at kildekoden til et dataprogram er gjort tilgjengelig (ofte på Internett) for alle. Det finnes mange forskjellige lisenser for åpen kildekode, men den mest brukte er GNU General Public License (GPL).
Oppdragsforhold	Et arbeidsforhold mellom en innleid og Norsk Helsenett som oppdragsgiver. Den innleide har ansettelsesforhold i en annen virksomhet enn Norsk Helsenett.
Personopplysningssikkerhet	Tiltak som beskytter mot utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet, jf personvernforordningen artikkel 4 nr. 12.
Personvernforordningen (GDPR)	Forordning om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger.
Personopplysning	Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet, jf. personvernforordningen (GDPR) artikkel 4 nr. 1.
Privilegerte brukerkontoer	Kontoer med spesielle rettigheter omfatter flere kategorier privilegerte kontoer: ▪ Kontoer med rot- eller administratorrettigheter på maskiner. ▪ Kontoer med spesielle privilegier i tjenester, systemer og applikasjoner ('superbrukere').

Begrep	Beskrivelse
Pseudonymisering	Å avidentifisere personopplysninger slik at de ikke kan knyttes til en bestemt person uten bruk av tilleggsopplysninger (for eksempel en koblingsnøkkel) som lagres adskilt og tilstrekkelig sikkert. Pseudonymiserte personopplysninger er ikke anonyme.
Registrert	En enkeltperson som personopplysninger kan knyttes til.
Relevante tredjeparter	Eksterne som driver behandling av data på vegne av Norsk helsenett eller Norsk helsenetts kunder.
Revisjonsplan	Alle tjenester skal ha en plan for revisjon av f.eks. autorisasjonsregister, risikovurderinger, sikkerhetsrevisjoner osv.
Risikoeier	Rollen risikoeier har ansvar for og myndighet til å styre risiko i en gitt tjeneste, informasjonssystem eller register.
RPO	Recovery Point Objective; Gjennopprettingsmål; handler om hvor mye data/ informasjon du ”tåler” å miste før det får store konsekvenser. Dette skal si oss noe om hvor ofte en trenger å ta sikkerhetskopi (backup)
RTO	Recovery Time Objective; Gjenopprettingstid; tidsrammen som systemer må gjenopprettes etter et brudd før det starter å få betydelige konsekvenser. Med andre ord, hvor lenge “går det greit” at systemet er nede. RTO vil i normale situasjoner alltid være lavere enn MTPD.
Samsvar	Etterlevelse av krav fra styringssystemet.
Sikkerhetsarkitektur	Et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenestene de tilbyr mot uautorisert tilgang, skade eller misbruk.
Sikkerhetsinstruks	De viktigste sikkerhets- og personvernreglene som alle ansatte (både interne og eksterne) skal forholde seg i det daglige.
Sikkerhetsklasse	Angir behov for konfidensialitet, integritet og tilgjengelighet.
Sikkerhetsklarert personell	Ansatt eller innleid som er sikkerhetsklarert av Sivil klareringsmyndighet.
Sikkert område (ift. sikkerhetsgradert informasjon)	Dedikert rom i NHNs lokaler i Trondheim hvor det kan behandles sikkerhetsgradert informasjon.

Begrep	Beskrivelse
Skadevare	Programvare som muliggjør uautorisert endring, sletting eller tilgang til opplysninger.
Skjermingsverdi	Når man aggregerer summen av alt denne nøkkelen skal kryptere, så vil denne nøkkelen være på det høyeste nivået. Handler om tilgangsstyring.
Skjermingsverdig informasjon	Informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.
Skjermingsverdig objekt	Begrep benyttet i sikkerhetsloven, og som eksempelvis betyr det fysiske området hvor all eller deler av skjermingsverdi infrastruktur er lokalisert.
Skjermingsverdig infrastruktur	Begrep benyttet i sikkerhetsloven, og som eksempelvis kan være komponentene og tjenestene som understøtter grunnleggende nasjonale funksjoner i henhold til sikkerhetsloven. Selve tjenesten eller komponentene inneholder ikke nødvendigvis skjermingsverdig informasjon.
Skjermingsverdig tjeneste	Se skjermingsverdig infrastruktur
Support	Løsningen har en gyldig support, hvor NHN selv eier supportavtalen eller hvor NHN er navngitt aktør på kundens supportavtale med 3. part.
SW	Software, også kalt programvare (Operativsystemer, Applikasjoner osv)
Taushetserklæring	En plikt alle ansatte og innleide har til å hindre at uautoriserte får tilgang til eller kjennskap til NHNs opplysninger slik definert i avtalen som regulerer taushetsplikten (taushetserklæringen).
Tjenesteutsetting eller utkontraktering	Utkontraktering, også omtalt som tjenesteutsetting eller konkurranseutsetting, (fra engelsk ”outsourcing”) går ut på at en organisasjon går over til å skaffe en vare eller tjeneste fra en ekstern leverandør i stedet for å levere denne selv. Forholdet mellom leverandør og bestiller reguleres av en kontrakt.
Toolkit	Et sett med verktøy, gjerne software komponenter, som tilbyr funksjonalitet til programvare / løsning som skal utvikles.
Tredjepartsleverandør	Virksomheter som bruker Helsenettet for å tilby sine egne tjenester, for eksempel journalleverandører som når sine kunder gjennom Helsenettet
Underdatabehandler	Underleverandører som behandler personopplysninger på vegne av databehandleren
Underleverandør	Underleverandør er leverandør til hovedleverandøren

Begrep	Beskrivelse
ISO/IEC 27001:2017	Ledelsessystem for informasjonssikkerhet - spesifiserer kravene for implementering av sikkerhetskontroll innen en individuell organisasjon. Den dekker også fysisk kontroll og IT-sikkerhetsspørsmål. Norsk tittel: ”Informasjonsteknologi - Sikringsteknikker - Ledelsessystemer for informasjonssikkerhet - Krav (ISO/IEC 27001:2013 innbefattet Cor 1:2014 og Cor 2:2015)”
Driftsmonitorering	Innhenting av logger fra tjenester og infrastruktur til bruk som grunnlag for å sikre kvalitet og oppetid i tjenesten.
Tilgangslogg	Logg over tilganger til informasjon, infrastruktur eller fysisk lokasjoner.