1. Informasjonssikkerhet i test

Dokumentsamlingen «Informasjonssikkerhet i test» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Informasjonssikkerhet i test», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Informasjonssikkerhet i test» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

Med Helse Nord menes hele foretaksgruppen med alle helseforetakene og det regionale helseforetaket.

Sikkerhetskravene omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Kravene som er beskrevet i dette dokumentet gjelder for all testing av IT-løsninger og IT-systemer som behandler helse- og personopplysninger og som skal kobles til IKT-infrastrukturen i Helse Nord. Se også sikkerhetsområdet «19 Sikkerhet i IKT produksjonsmiljø».

3. Formål

Kravene i dette dokumentet skal sikre at informasjonssikkerhet blir ivaretatt i Helse Nords testprosesser og alle ulike testmiljø, i tråd med til enhver tid gjeldende regelverk innen informasjonssikkerhet.

Dette gjelder både testmiljø og QA-miljø. Helse Nord IKT sitt testsenter er *ett* slikt testmiljø. Dette benevnes heretter som Helse Nord IKTs Testsenter. Kravene gjelder også for testing som foregår i andre testmiljø og i alle utviklingsmiljø i Helse Nord.

Kravene gjelder også bruken av testdata, for å ivareta personvern og informasjonssikkerhet for direkte og/eller indirekte identifiserbare helse- og personopplysninger brukt ved testing.

Kravene skal sikre akseptabel risiko og forhindre uønsket påvirkning mellom alle testmiljø, inkludert QA-miljø, og produksjonsmiljø.

Kravene knyttet til testing skal bidra til å forhindre, samt begrense omfang og konsekvenser, av eventuelle sikkerhetshendelser i produksjon.

4. Sikkerhetskrav

4.1 Informasjonssikkerhet i testmiljø

4.1.1 Helse Nords retningslinjer og prosedyrer for tilgangsstyring, sikring av konfidensialitet og integritet for produksjonsmiljø gjelder også for miljø som benyttes til testing

a) Der det er nødvendig å teste integrasjoner mot andre systemer, skal disse systemene og integrasjonene som hovedregel også etableres i testmiljøet.
b) Dersom integrasjoner ikke kan testes i testmiljø, må risiko relatert til personvern og informasjonssikkerhet vurderes og risikoreduserende tiltak foreslås/iverksettes om nødvendig. Avviket/unntaket skal godkjennes av dataansvarlig eller den som dataansvarlig utpeker. De som bestiller testingen er også ansvarlig for at risikovurdering blir gjennomført.

4.2 Informasjonssikkerhet i forbindelse med testing

4.2.1 Testing skal ikke påvirke informasjonssikkerheten i produksjonsmiljøet

a) Miljøer i Helse Nord IKTs Testsenter skal etableres på separate nettverk atskilt fra produksjon.
b) Det skal være en separat brukerkatalog for Helse Nord IKTs Testsenter.
c) Det skal ikke være mulig å utilsiktet få tilgang til helse- og personopplysninger i produksjon via et testmiljø.
d) Det skal ikke være mulig å endre helse- og personopplysninger i produksjon via et testmiljø.
e) Det skal som hovedregel utføres verifikasjon i et produksjonslikt miljø før produksjonssetting, for å sikre at nye systemer og oppgraderinger ikke påfører skade på produksjonsmiljøet, og for å sikre at nye systemer og oppgraderinger fungerer på en korrekt og sikker måte.
f) Tilgang til testmiljø skal godkjennes av de som eier testmiljøet.
g) Kun klienter som oppfyller Helse Nords sikkerhetskrav skal kunne kople seg opp mot testmiljøene.
h) Alle nye testmiljø skal som hovedregel plasseres innenfor Helse Nord IKTs Testsenter. Unntak må godkjennes av dataansvarlig, basert på risikovurdering med begrunnelse for avviket fra de som har bestilt testen.

4.2.2 Tilstrekkelig informasjonssikkerhet og personvern skal ivaretas ved testing

a) Dataansvarlig og databehandler for systemet eller tjenesten som skal testes, har ansvar for at testing gjennomføres i henhold til gjeldende krav og retningslinjer for informasjonssikkerhet.
b) Brukeroppslag på identifiserbare helse- og personopplysninger skal logges og loggene skal være tilgjengelige for dataansvarlig.
c) Dataansvarlig og databehandler har ansvar for at de som er involvert i testingen
    - sikres nødvendig opplæring i eller har kunnskap om sikkerhetstesting, innebygd personvern og sikkerhet.
    - **gjøres kjent med eller involveres i risikovurderinger som er relevante for å kunne vurdere hvilke testmiljø og testdata som skal benyttes.**
    - **gjøres kjent med at de skal vurdere hvilke sikkerhetskrav og -funksjonalitet som bør testes.**

4.2.3 Testing av sikkerhetskrav og krav til personvern skal ivaretas

a) Funksjonalitet for å ivareta konfidensialitet, integritet og sporbarhet skal testes for systemer og løsninger som behandler helse- og personopplysninger.
b) Det skal sjekkes at tiltak fra eventuelle personvernkonsekvensvurderinger er implementert og fungerer etter hensikten.

4.3 Informasjonssikkerhet ved bruk av testdata

4.3.1 Testing skal i størst mulig grad gjøres på syntetiske data / ikke-personidentifiserbare data. Formålet er å begrense bruk av personidentifiserbare data ved testing til et minimum

a) Anonymisering skal gjøres i samsvar med veileder om anonymisering av personopplysninger fra Datatilsynet https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/hvordan-anonymisere-personopplysninger/.
b) Direkte eller indirekte personidentifiserbare data skal kun brukes til testing der det ikke er mulig å oppnå tilstrekkelig testkvalitet ved bruk av syntetiske og/eller anonymiserte data. I slike tilfeller skal bruk av personidentifiserbare data begrenses.
c) Ved testing på personidentifiserbare data skal det gjøres en dokumentert vurdering av formålet med testingen. De som bestiller testingen skal gjøre vurdering av personvernkonsekvenser og risiko før testing gjennomføres, samt tiltak for å minimere bruk av personopplysninger. Dette skal godkjennes av dataansvarlig, basert på risikovurdering med begrunnelse fra de som har bestilt testen.

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

1. ISO 27002: A.14: System acquisition, development and maintenance
2. Lov om behandling av personopplysninger («personopplysningsloven» https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysningsloven)

3. EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL).
4. Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet
5. Datatilsynets veileder for programvareutvikling med innebygd personvern https://www.datatilsynet.no/regelverk-og-skjema/veiledere/programvareutvikling-med-innebygd-personvern/

- Sjekkliste for krav https://www.datatilsynet.no/globalassets/global/regelverk/veiledere/innebygd-personvern/02-sjekkliste_krav_250817.pdf

6. Datatilsynets veileder om grunnleggende personvernprinsipper https://www.datatilsynet.no/regelverk-og-skjema/veiledere/grunnleggende-personvernprinsipper-etter-nytt-regelverk/?id=7770
7. Datatilsynets veileder om anonymisering av personopplysninger https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/hvordan-anonymisere-personopplysninger/