

**<Navn på virksomheten>**

**Rapportering for perioden: <01.09.20xx – 31.08.20xx >**

Ledelsens gjennomgang

Innhold

[1 Introduksjon 3](#_Toc75166894)

[1.1 Formål 3](#_Toc75166895)

[1.2 Om rapporten 3](#_Toc75166896)

[2 Oversikt – Ledelsens gjennomgang 4](#_Toc75166897)

[2.1 Ansvar og organisering 4](#_Toc75166898)

[2.2 Risikovurderinger 5](#_Toc75166899)

[2.3 Personvernkonsekvensvurderinger (DPIA) 6](#_Toc75166900)

[2.4 Avvik og hendelser 7](#_Toc75166901)

[2.5 Revisjon, tilsyn, mv. 8](#_Toc75166902)

[2.6 Oppfølging av avtaler og leverandører 9](#_Toc75166903)

[2.7 Norsk helsenett 10](#_Toc75166904)

[3 Prioriteringer og konklusjon 11](#_Toc75166905)

[3.1 Status for prioriteringer forrige periode 11](#_Toc75166906)

[3.2 Prioriteringer neste periode 11](#_Toc75166907)

[3.3 Ledelsens konklusjon 12](#_Toc75166908)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Godkjent av: |  | | | U.off: |  | Saksbehandler: | |  | | |
| Godkjent dato: |  | | Versjon: |  | Sak- og dokumentnr: | |  | | | |
| Mal – denne versjonen: | | Ledelsens gjennomgang (2022) | | | Erstatter mal: | Ledelsens gjennomgang (2021) | | | Eier: | FIN |

# Introduksjon

## Formål

Ledelsens gjennomgang skal sikre at ledelsen får en helhetlig oversikt over personvern- og informasjonssikkerhetsarbeidet i virksomheten, og er en aktivitet for å følge opp, forbedre og effektivisere styringen av dette arbeidet. Formålet med gjennomgangen er å vurdere om status på virksomhetens arbeid med informasjonssikkerhet og personvern er tilfredsstillende. Gjennomgangen gir ledelsen grunnlag for prioriteringer og beslutninger som sikrer kontinuerlig forbedring i det systematiske arbeidet. Ledelsens gjennomgang skal også bidra til å fremskaffe nødvendig grunnlag for utfylling av «Virksomhetsleders egenerklæring».

Ledelsens gjennomgang av informasjonssikkerhet er forankret i Instruks for informasjonssikkerhet punkt 3.6 for Oslo kommune (byrådssak 1105/13) og gjennomføres årlig.

*«Informasjonssikkerhet skal være gjenstand for oppfølgning, regelmessig kontroll og revisjon for å sikre etterlevelse, både internt i den enkelte virksomhet og fra overordnet nivå. Herunder skal ledelsen i den enkelte virksomhet årlig foreta en gjennomgang av informasjonssikkerheten i virksomheten.»*

Ledelsens gjennomgang er i tillegg et krav i Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen, kap 2.5) for virksomheter som er knyttet til Norsk helsenett.

Rapportering gjennom LG er knyttet til virksomhetens aktiviteter innen informasjonssikkerhet og personvern. Dette dokumentet gir en overordnet oversikt og status for siste periode, og setter føringer for videre aktiviteter og prioriteringer.

## Om rapporten

|  |
| --- |
| **Sett inn rapporteringsperiode, dersom denne avviker fra 01.09.2021 – 31.8.2022:** |
|  |
| **Involverte som har bidratt med informasjon til, og utfylling av, rapport:** |
|  |
| **Datakilder og datagrunnlag:** |
|  |

# Oversikt – Ledelsens gjennomgang

## Ansvar og organisering

|  |
| --- |
|  |
| **Gi en overordnet beskrivelse av hvordan arbeidet med informasjonssikkerhet og personvern er organisert i virksomheten.** |
|  |
| **Beskriv eventuelle endringer i organisering av arbeidet med personvern og informasjonssikkerhet som er gjort i rapporteringsperioden.** |
|  |
| **Gi en kort vurdering av om valgt personvern- og informasjonssikkerhetsorganisering fungerer etter hensikten.** |
|  |
| **Gi en kort vurdering av om virksomheten har tilstrekkelige ressurser til personvern- og informasjonssikkerhetsarbeidet.** |
|  |

## Risikovurderinger

Risikovurderinger innen informasjonssikkerhetsområdet som er gjennomført i perioden.

| **Nr.** | **Beskrivelse av risiko- vurderinger** | **Risiko-vurderingens avgrensning** | **Beskrivelse av funn (mulig uønsket hendelse)** | **Vurdering alvorlighet** | | | **Planlagte tiltak** | **Status / restrisiko** | **Ansvarlig** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |
| **1** |  |  |  |  | | | 1.1 |  |  |
|  |  |  |  |  | | | 1.2 |  |  |
|  |  |  |  |  | | |  |  |  |
| **2** |  |  |  |  | | | 2.1 |  |  |
|  |  |  |  |  | | | 2.2 |  |  |
| **3** |  |  |  |  | | |  |  |  |
|  |  |  |  |  | | |  |  |  |
|  | ***Kommentar:*** *<Beskrivelse av systematikk og strategi for å velge risikovurderinger er ønsket her.>* | | | | | | | | |

## Personvernkonsekvensvurderinger (DPIA)

Personvernkonsekvensvurderinger (DPIA) etter GDPR art 35 som er gjennomført i perioden. DPIA er påkrevd når risikoen for den registrertes rettigheter og friheter anses som høy.

| **Nr.** | **Beskrivelse av DPIA: kort om bakgrunn og hvilken løsning/systemer som er vurdert** | **DPIAs omfang og avgrensning** | **Vurdering alvorlighet** | | |
| --- | --- | --- | --- | --- | --- |
|  |  |  |
| **1** |  |  |  | | |
| **2** |  |  |  | | |
| **3** |  |  |  | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nr.** | **Beskrivelse av funn** | **Beskrivelse av tiltak** | **Status/restrisiko** | **Forhåndsdrøftelse med Datatilsynet (Ja/Nei)** | **Ansvarlig** |
| **1** |  |  |  |  |  |
| **2** |  |  |  |  |  |

## Avvik og hendelser

Avvik og hendelser som er registrert i perioden. Dette kan være helt eller delvis bortfall av kritiske tjenester, fare for liv og helse, og personopplysninger på avveie slik at uautoriserte har fått eller kan få tilgang. Avvik omfatter også brudd på personopplysningssikkerhet etter GDPR.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr.** | **Beskrivelse av avvik/hendelse** | **Beskrivelse av årsak** | **Vurdering alvorlighet** | | | **Planlagte tiltak?** | **Status** | **Meldt til Datatilsynet (Ja/Nei)** | **Informasjon gitt til de berørte registrerte?** | **Ansvarlig** |
|  |  |  | (Gjelder ved brudd på personopplysningssikkerhet) | |
| **1** |  |  |  | | |  |  |  |  |  |
| **2** |  |  |  | | |  |  |  |  |  |
| **3** |  |  |  | | |  |  |  |  |  |
| **4** |  |  |  | | |  |  |  |  |  |
| **Kommentar:** <Beskrivelse av kjente sårbarheter eller sikkerhetsmessige mangler er ønsket her.> | | | | | | | | | | |

## Revisjon, tilsyn, mv.

Rapportering av enkeltvis og systematiske tiltak som er gjennomført for å kontrollere om virksomheten etterlever gjeldende krav innenfor informasjonssikkerhets- og personvernområdet. Tiltakene som listes opp kan være for ekstern eller intern implementering.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr.** | **Beskrivelse av revisjon, tilsyn, mv.** | **Aktivitetens omfang/formål/fokus** | **Hovedfunn** | **Vurdering alvorlighet** | | | **Planlagte tiltak** | **Status** | **Ansvarlig** |
|  |  |  |
| **1** |  |  |  |  | | |  |  |  |
| **2** |  |  |  |  | | |  |  |  |
| **3** |  |  |  |  | | |  |  |  |
| **Kommentar:** | | | | | | | | | |

## Oppfølging av avtaler og leverandører

Oppsummering av kontroll og oppfølging av inngåtte avtaler, inkl. databehandleravtaler, og av leverandørers etterlevelse av personvern- og informasjonssikkerhetskrav.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr.** | **Avtale/leverandør** | **Vurdering / endringsbehov for avtale** | **Leverandørs etterlevelse av PV-og ISkrav** | **Vurdering alvorlighet** | | | **Planlagte tiltak** | **Status** | **Ansvarlig** |
|  |  |  |
| **1** |  |  |  |  | | |  |  |  |
| **2** |  |  |  |  | | |  |  |  |
| **3** |  |  |  |  | | |  |  |  |
|  |  |  |  |  | | |  |  |  |
|  |  |  |  |  | | |  |  |  |
| **Kommentar:** <Beskrivelse av systematikk og strategi for å velge hvilke avtaler som gjennomgås, er ønsket her> | | | | | | | | | |

## Norsk helsenett

Dette avsnittet er kun relevant for virksomheter som er tilknyttet Norsk helsenett. Dersom virksomheten har utført kontrollaktiviteter som kan være av betydning for samsvar med Normen og tilknytning til Norsk helsenett, så skal disse listes opp i tabellen under.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr.** | **Utført kontrollaktivitet** | **Eventuelle behov for endringer eller nye tiltak** | **Vurdering alvorlighet** | | | **Planlagte tiltak** | **Status** | **Ansvarlig** |
|  |  |  |
|  |  |  |  | | |  |  |  |
|  |  |  |  | | |  |  |  |
|  |  |  |  | | |  |  |  |
| **Kommentar:** | | | | | | | | |

# Prioriteringer og konklusjon

## Status for prioriteringer forrige periode

Oppdatert status for aktiviteter besluttet i forrige Ledelsens gjennomgang.

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | **Forrige periodes prioriteringsområde** | **Status** | **Ansvarlig** |
| **1** |  |  |  |
| **2** |  |  |  |
| **3** |  |  |  |

## Prioriteringer neste periode

Oversikt over aktiviteter ledelsen ønsker å prioritere for neste periode.

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | **Prioriteringsområde** | **Begrunnelse** | **Ansvarlig** |
| **1** |  |  |  |
| **2** |  |  |  |
| **3** |  |  |  |

## 

## Ledelsens konklusjon

*<Oppsummering fra virksomhetens leder.* Konklusjonen skal gi føringer for videre arbeid med personvern og informasjonssikkerhet i virksomheten og supplere listen over prioriterte tiltak *>*