[ [FORSIDE](http://xn--designverkty-5jb.oslo.kommune.no/) ]

Informasjon om malen

*Denne malen for risikovurderingsrapport er et hjelpemiddel som Byrådsavdeling for finans gjør tilgjengelig for virksomhetene i Oslo kommune.*

*Malen er frivillig å benytte og kan ansees som en skisse som virksomhetene kan tilpasse i henhold til behov i virksomhetene.*

*Veiledning i malen er skrevet i kursiv og innenfor klammeparenteser. Veiledningstekst slettes før rapport ferdigstilles.*

*Rapporter basert på denne malen kan inneholde sensitiv informasjon om sårbarheter i virsomhetsprosesser og/eller systemer mm. Alvorligheten vil være avhengig av blant annet hva slags type informasjonen som behandles i prosess eller system, og formålet med prosessen eller systemet. Rapporten bør derfor, etter vurdering av hva som er risikovurdert, eventuelt merkes med U.off. eller klassifisering av konfidensialitet iht. klassifiseringsregimet i virksomheten. Rapporten bør også lagres og overføres med nødvendige beskyttelsestiltak avhengig av risiko dersom innholdet blir kjent for uvedkommende.*

*Rapporten skal som minimum distribueres til, eventuelt gjøres tilgjengelig for, leder som er ansvarlig for vurdert prosess, til systemeier(e) og systemforvalter(e) og til de personene som har fasilitert risikovurderingen.*

*Rapporten bør distribueres til virksomhetsleder, og den må distribueres til virksomhetsleder dersom det etter tiltak fortsatt finnes uakseptabel risiko (hendelser i «rød sone»).*

*Rapporten distribueres til andre bidragsytere i risikovurderingen etter behov.*

<Navn på systemet eller prosessen som er risikovurdert>

# Dokumentasjon, ajourhold og distribusjon

|  |  |
| --- | --- |
| **Grunnleggende informasjon** | |
| System- eller prosessnavn |  |
| Tidspunkt for start av risikovurdering |  |
| Ansvarlig (System- eller prosesseier) |  |
| Eventuelle vedlegg, f.eks regnearkverktøy for risikovurdering |  |
| Saksnummer (hvis relevant) |  |

Tabell 1 Grunnleggende informasjon

|  |  |  |
| --- | --- | --- |
| **Endringshistorikk** | | |
| Dato for første versjon av ROS | |  |
| Evt. dato for oppdatering | Endringer | Godkjent av eier |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Tabell 2 Endringshistorikk

|  |  |
| --- | --- |
| **Distribusjon** | |
| Ansvarlig leder |  |
| Systemeier |  |
| Fasilitator(er) av risikovurdering |  |
| Systemforvalter |  |
| Virksomhetsleder |  |
| Andre bidragsytere |  |

Tabell 3 Distribusjon av rapport

Innhold

[1 Dokumentasjon, ajourhold og distribusjon 3](#_Toc101428418)

[2 Innledning 5](#_Toc101428419)

[2.1 Bakgrunn 5](#_Toc101428420)

[2.2 Mål for risikovurderingen 5](#_Toc101428421)

[2.3 Omfang 5](#_Toc101428422)

[2.4 Avgrensninger 5](#_Toc101428423)

[3 Metodikk 6](#_Toc101428424)

[4 Underlag 6](#_Toc101428425)

[5 Gjennomføring 6](#_Toc101428426)

[5.1 Deltakere 6](#_Toc101428427)

[5.2 Møter og workshoper 6](#_Toc101428428)

[5.3 Områder behandlet 7](#_Toc101428429)

[5.4 Uønskede hendelser 8](#_Toc101428430)

[6 Oppsummering av identifisert risiko 8](#_Toc101428431)

[7 Risikohåndtering 9](#_Toc101428432)

[7.1 Identifiserte tiltak 9](#_Toc101428433)

[7.2 Risiko etter tiltak 9](#_Toc101428434)

[8 Godkjenning av restrisiko 10](#_Toc101428435)

# Innledning

## Bakgrunn

*<Beskriv hvorfor denne risikovurderingen er gjennomført. Nytt system eller prosess? Regelmessig oppdatering?>*

## Mål for risikovurderingen

Mål for risikovurderingen har vært å: (stryk det som ikke passer)

* Foreta en vurdering av verdiene i <System / prosess>
* Identifisere trusler og sårbarheter som er relevante for <System / prosess>
* Analysere uønskede hendelser på prioriterte områder i bruk, drift og forvaltning av <System / prosess>
* Indentifisere mulige tiltak for å redusere risiko knyttet til de uønskede hendelsene, til akseptabelt nivå.
* Kostnadsestimere og vurdere effekt av foreslåtte tiltak
* Sette prioritet på tiltakene
* Beslutte hvilke tiltak som skal gjennomføres
* Tilordne ansvarlige avdelinger / roller for gjennomføring av tiltakene
* Dokumentere at risiko er håndtert

## Omfang

Risikovurderingen omfattet analyser av: (stryk eller legg til)

* Hele eller deler av virksomhetsprosesser
* Spesifikke funksjoner eller oppgaver
* Hele eller deler (komponenter) av system
* Spesifikke grensesnitt
* Ende-til-ende sikring
* Aktuelle områder fra tilpasset trusselbilde
* Roller og ansvar for informasjonssikkerhet
* Forvaltningen av <System(er)>
* Tilgangsstyring
* Endringshåndtering
* Avtaleverk med leverandører/underleverandører>

## Avgrensninger

*<Ved behov: Liste opp eller beskrive områder som ikke er dekket innenfor omfang. Gi om ønskelig referanser til tidligere utførte risikovurderinger av komponenter eller funksjoner som er tatt ut.>*

# Metodikk

*<Beskrivelse av metodikk som er benyttet. For eksempel:*

*«Risikovurderingen er gjennomført med metodikk og verktøy som er lagt ut på Oslo kommunes felles intranett under valget «Informasjonssikkerhet og personvern».*

*Risikovurderingen er hovedsakelig gjennomført gjennom risikoworkshops med deltakere fra ulike organisatoriske enheter i Oslo kommune og med ulike erfaringer med <system / prosess.»>*

# Underlag

Følgende dokumentasjon er benyttet som underlag til risikovurderingen

* <Liste over viktig mottatt dokumentasjon>

# Gjennomføring

## Deltakere

Følgende personer har bidratt i risikovurderingen

|  |  |  |
| --- | --- | --- |
| **Organisasjon** | **Rolle** | **Navn** |
|  | Systemeier |  |
|  | Systemforvalter |  |
|  | Sikkerhetsansvarlig |  |
|  | IT-drift |  |
|  | Sikkerhetsarkitekt |  |
|  | Bruker |  |
|  | <andre> |  |

Tabell 4 Deltakere

## Møter og workshoper

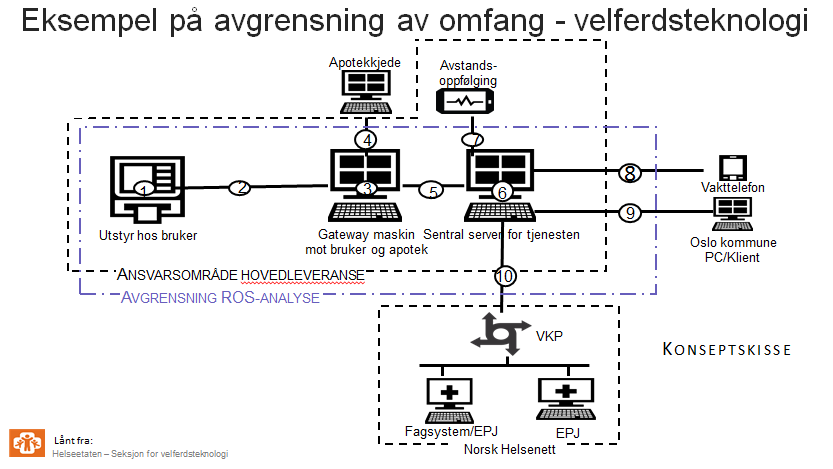
Følgende risikoworkshops og møter har vært gjennomført *<Eksempel>*:

|  |  |
| --- | --- |
| **Dato** | **Type** |
| 1. januar 2021 | Verdi-/trusselvurderingsmøte |
| 1. januar 2021 | Risikovurderingsworkshop |
| 1. januar 2021 | Risikohåndteringsworkshop |

Tabell 5 Oversikt over møter gjennomført

## Områder behandlet

*<Her bør det linkes til eller legges inn en beskrivelse/figur av systemet som viser komponenter, grensesnitt, kommunikasjonslinjer, aktører osv. Det er nyttig å nummerere komponenter og grensesnitt/kommunikasjonslinjer og beskrive hvert element i en tabell under figuren. Det er også nyttig om figuren viser avgrensningen av hva som omfattes av ROS-analysen>*

**

*Figur 1 Eksempel på avgrensning av omfang*

|  |  |  |
| --- | --- | --- |
| **ID** | **Forklaring** | **Merknader** |
| **1** | Utstyr plassert hos bruker av velferdsteknologi | IoT-basert teknologi levert av leverandør X. |
| **2** | Kommunikasjonslinje mellom sentral server (via gateway) for varsler mm | Kryptert forbindelse basert på xx-teknologi. |
| **3** | Eget utstyr som brukes som gateway både mot apotek som leverer medisiner og mot skytjenesteleverandør | Basert på xx-teknologi levert av leverandør X. |
| **4** | osv |  |

Tabell 6 Forklaring til komponenter og grensesnitt i figuren

Tema som er diskutert: (stryk det som ikke passer eller legg til)

* Organisering av informasjonssikkerhet
* Håndtering av personopplysninger av særlige kategorier
* Tilgangsstyring
* Kontroll av tilganger og tilgangsstyring
* Logging
* Dokumentasjon
* Personell
* Drift/driftsrutiner, nettverk
* Testing og testrutiner
* Oppdatering av programvare
* Integrasjon mot andre systemer
* Leverandører
* Hendelseshåndtering, forbedringer
* Kontinuitet
* Samsvar med lover og annet regelverk

## Uønskede hendelser

Følgende uønskede hendelser ble vurdert i ROS-analysen:

|  |  |
| --- | --- |
| **Risiko ID** | **Uønsket hendelse** |
| **R1** |  |
| **R2** |  |
| **R3** |  |
| **R4** |  |

Tabell 7 oversikt over uønskede hendelser vurdert

# Oppsummering av identifisert risiko

Identifiserte risikoer og forslag til tiltak for å redusere risiko til akseptabelt nivå er dokumentert i vedlegg X.

Det ble i risikovurderingen identifisert <xx> uønskede hendelser. <yy> av disse ble vurdert som høy risiko (røde), <zz> ble vurdert som middels risiko (gule), og <ææ> ble vurdert som lav risiko (grønne).

Fordelingen av uønskede hendelser med hensyn på konsekvens og sannsynlighet (risikoer før tiltak) kan sees i risikomatrisen nedenfor.

*<sett inn risikomatrise (5x5)>*

Følgende uønskede hendelser ble vurdert til høy risiko:

* <Hendelse a>
* <Hendelse b>

# Risikohåndtering

## Identifiserte tiltak

Det ble identifisert totalt <antall> risikoreduserende tiltak. Disse ble prioritert etter følgende kriterier:

* Prioritet 1: Tiltaket skal gjennomføres snarest
* Prioritet 2: Tiltaket skal gjennomføres ved anledning
* Prioritet 3: Tiltaket prioriteres ikke

*<Ved anledning bør spesifiseres. F.eks. før produksjonssetting av løsning, før gjennomføring av pilot, e.l.>*

Følgende tiltak har prioritet 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltak** | **Utføres av** | **Utføres innen** | **Utført?** |
|  |  |  |  |
|  |  |  |  |

Tabell 8 Prioritet 1 tiltak

Følgende tiltak har prioritet 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltak** | **Utføres av** | **Utføres innen** | **Utført?** |
|  |  |  |  |
|  |  |  |  |

Tabell 9 Prioritet 2 tiltak

## Risiko etter tiltak

Følgende risikomatrise viser restrisiko, dvs risiko etter at identifiserte tiltak er gjennomført:

*<Sett inn 5x5 matrise som viser risiko etter tiltak>*

# Godkjenning av restrisiko

Beskrevet høy og moderat risiko aksepteres.

* <sett inn liste>

<signatur besluttende leder> <sted og dato>