



KiNS

foreningen kommunal
informasjonssikkerhet

Ressursbank for risiko og tiltak

21. April 2022



Velkommen til KiNS ressursbank

Denne ressursbanken er ment til å dele risikoscenarier og risikoreduserende tiltak slik at ikke alle må tenke ut de samme hendelsene på egen hånd. Scenariene og tiltakene skal være til refleksjon og inspirasjon for å hjelpe personer som behandler personopplysninger i det daglige, men som ikke er vant til å gjøre risikovurderinger.

I oversikten over risikoscenarier kan det søkes og filtreres, og de forskjellige scenariene har også knyttet til seg relevante tiltak man kan finne ved å trykke på øye-ikonet ved siden av scenariet.

34

PERSONVERNKONSEKVENSVURDERING...

41

RISIKO- OG SÅRBARHETSANALYSE (ROS)

16

RISIKOREDUSERENDE TILTAK

Risikoscenarier



Risiko scenarier ?

↻ 30 ☰FILTER ▾Viser 1 til 30 av 41stkREGISTRER

HENDELSE	ÅRSAK	BESKRIVELSE	VALG
Beskyttelsesverdige opplysninger blir tilgjengelig for uvedkommende	Passord på avveie	Ansatte deler med andre (feks barn). Uvedkommende får tak i ansattes passord.	 
Svindel og ID-tyveri			

Filtrering



Risiko scenarier ?

 30 FILTER 

Viser 1 til 2 av 2stk

REGISTRER

Hendelse

BRUDD PÅ LOVLIGHET 

Sektor

ALLE 

Kategori

ALLE 

Relevans

DPIA 

Vis maler

NEI 

Eksempel nr. 1



Opplysninger blir
tilgjengelig for
uvedkommende

Brudd på lovlighet

Brudd på
ansvarlighet

Ansatt sender
brev/informasjon til feil
mottaker

Bruker/tjenestemottaker får utilsiktet innsyn i andre personers helse- og personopplysninger. Brudd på taushetsplikten.



Eksempel nr. 1



ENDRE

Generelt

Navn

Ansatt sender brev/informasjon til
feil mottaker

Kategori

- Konfidensialitet
- Personvernprinsippene

Sektor

•

Relevans

- ROS
- DPIA

Beskrivelse

Bruker/tjenestemottaker får utilsiktet innsyn i andre personers helse- og personopplysninger. Brudd på taushetsplikten.

Risikoreduserende tiltak

Eksempel nr. 1 - tiltak



Risikoreduserende tiltak

Opplæring

Basic

Opplæring av ansatte i personvernreglene og/eller informasjonssikkerhet

[Les mer >](#)

Gjennomgang av prosedyre for opplæring

Basic

Er prosedyren for opplæring tilfredsstillende? Må den ansatte kvittere for at opplæring er gjennomført? Er det godt nok oppfølging av at den ansatte gjennomfører pålagt opplæring?

[Les mer >](#)

Etablere/revidere rutine som skal sikre at informasjon kommer til rett person

Basic

Hvordan legge til rett mottaker i fagsystem/sakssystem. Virksomheten bør benytte til kontakt- og reservasjonsregistret for utsending av brev hvis den har tilgang til dette.

[Les mer >](#)

Filtrering nr. 2



Risiko scenarier ?

Søk

↻ 30 ☰

FILTER ^

Viser 1 til 6 av 6stk

REGISTRER

Hendelse

OPPLYSNINGER BLIR TILGJENGELIG FOR U

Sektor

ALLE

Kategori

ALLE

Relevans

DPIA

Vis maler

NEI

Eksempel nr. 2



Opplysninger blir tilgjengelig
for uvedkommende

Ødeleggelse av data

Tap av data

Snoking og misbruk av
tilgang til informasjon

Brudd på ansvarlighet

Mangelfull tilgangsstyring

Kan ha mange underliggende årsaker, hvilket nivå skal vi legge oss på?
Prosess - brukere som ikke slettes når arbeidsforhold opphører eller endres
Manglende bruk av sterk autentisering
Svak eller manglende passord-policy



Eksempel nr. 2



ENDRE

Generelt

Navn

Mangelfull tilgangsstyring

Kategori

- Konfidensialitet
- Integritet
- Personvernprinsippene

Sektor

•

Relevans

- ROS
- DPIA

Beskrivelse

Kan ha mange underliggende årsaker, hvilket nivå skal vi legge oss på ?

- Prosess - brukere som ikke slettes når arbeidsforhold opphører eller endres
- Manglende bruk av sterk autentisering
- Svak eller manglende passord-policy

Eksempel nr. 2 - tiltak



Risikoreduserende tiltak

Krav om sterk autentisering (MFA)

Professional

[Les mer >](#)

NSM 2.6.2 - Etabler en formell prosess for administrasjon av kontoer, tilganger og rettigheter

Basic

Etabler en formell prosess for administrasjon av kontoer, tilganger og rettigheter. a) Prosessen bør omhandle i) kontoer til brukere, enheter og systemprosesser, ii) tilganger til systemer og applika...

[Les mer >](#)

NSM 2.6.1 - Etabler retningslinjer for tilgangskontroll

Professional

Etabler retningslinjer for tilgangskontroll. a) Retningslinjene bør dekke flest mulig av ressursene i virksomheten: brukere, klienter, felles-mapper, server-applikasjoner, servere, nettverksenheter, ...

[Les mer >](#)

NSM 2.6.3 - Benytt et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter

Professional

Benytt et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter. a) Styr kontoer, tilganger og rettigheter til flest mulig av ressurser (ref. 2.6.2.a) i virksomheten m...

[Les mer >](#)



Velkommen til KiNS ressursbank

Denne ressursbanken er ment til å dele risikoscenarier og risikoreduserende tiltak slik at ikke alle må tenke ut de samme hendelsene på egen hånd. Scenariene og tiltakene skal være til refleksjon og inspirasjon for å hjelpe personer som behandler personopplysninger i det daglige, men som ikke er vant til å gjøre risikovurderinger.

I oversikten over risikoscenarier kan det søkes og filtreres, og de forskjellige scenariene har også knyttet til seg relevante tiltak man kan finne ved å trykke på øye-ikonet ved siden av scenariet.

34

PERSONVERNKONSEKVENSVURDERING...

41

RISIKO- OG SÅRBARHETSANALYSE (ROS)

16

RISIKOREDUSERENDE TILTAK