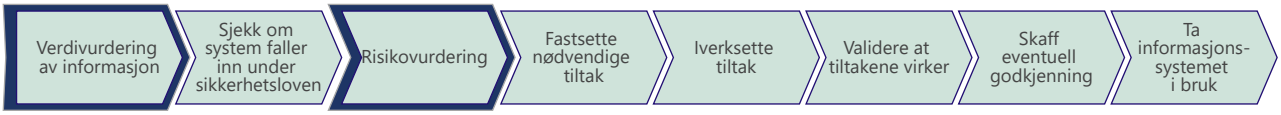
Innføre nytt IT system



Innføre nytt informasjonssystem

Prosesseier: Ole Jakob Ottestad | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 27.9.2023 | Publisert versjon: 1

Hensikt:

I de tilfellene da et nytt informasjonssystem skal innføres må det gjennomføres en strukturert prosess for å sikre at innføringen i NND overholder gjeldende lover, reguleringer og regler og at tiltak for sikring ivaretar verdiene som informasjonssystem skal behandle/forvalte.

Omfang:

Prosessen gjennomføres hver gang det skal innføres et nytt informasjonssystem. Prosessen blir typisk utført som del av en prosjektgjennomføring og vil variere i omfang avhengig av om systemet som skal tas i bruk behandler verdier som faller under sikkerhetsloven/virksomhetssikkerhetsforskriften eller ikke.

Prosessen skal gjennomføres også for systemer som ikke faller under sikkerhetsloven/virksomhetssikkerhetsforskriften for å sikre at nødvendige tiltak knyttet til informasjonssikkerhet er vurdert og satt i drift før systemet tas i bruk. Det skal spesielt vurderes og tas hensyn til behandling av personopplysninger som gjøres i systemet i verdivurderingen og risikoanalysen.

Prosessen skal gjennomføres uavhengig av driftsformen for systemet og gjelder dermed også for innføring av rene sky-baserte løsninger i tillegg til løsninger som driftes helt eller delvis av NNDs organisasjon.

Merk at prosessen kommer i tillegg til nødvendige aktiviteter knyttet til prosessene beskrevet under «Drift og forvaltning av IT» som omhandler krav til behandling i IT arkitekturstyring og håndtering IT endringer, testing og verifikasjon og håndtering av utrulling.

Resultat

NND har iverksatt nødvendige tiltak og innhentet nødvendige godkjenninger før informasjonssystem settes i drift.

Roller og rollenes ansvar i prosessen

Utførende roller i prosessen	***Rollens oppgaveansvar/myndighet i denne prosessen***
Systemeier	Systemeier står ansvarlig for at prosessen gjennomføres ved innføring av nytt system. De praktiske oppgavene kan delegeres til prosjektleder eller andre i ordinær linjeorganisasjon avhengig av organisering av arbeidet.
Fagansvarlig Forebyggende sikkerhet	Skal involveres i risikoanalyser og i eventuell søknad om godkjenning av å ta systemet i bruk

Eksterne krav/føringer til prosessen:

Kravdokument (lovverk, standarder o.l.)	***Kapittel, paragraf e.l.***
Lov om nasjonal sikkerhet (SIK)	Kapittel 6
Virksomhetssikkerhetsforskriften (VSF)	
Lov om behandling av personopplysninger (GDPR)	

Virksomhetskrav:

Kravdokument
Politikk for sikkerhet
Strategi for virksomhetsstyring
Delstrategi for IT

Dokumentert informasjon (styrende dokumentasjon)

Instruks

Instruks for informasjonssikkerhet

Prosedyre

Prosedyre for å dokumentere sikkerhetskrav til skjermingsverdig informasjonssystem

Veiledning

Brukerveiledning dokumentasjon av gradert informasjonssystem

Maler

Sjekkliste

Sjekkliste overlevering til IT drift

Linker

Prosess - Drifte IT løsninger

Prosess - Verdivurdering av informasjon

Verdivurdering av informasjon

Prosesseier: Ole Jakob Ottestad | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 9.2.2024 | Publisert versjon: 1

Gjennomfør verdivurdering knyttet til den informasjonen som IT systemet skal behandle, eventuelt knyttet til de objektene som IT systemet skal styre. Verdivurderingen skal benyttes som basis for å avgjøre hvilke behandlingsregler som må ivaretas for IT systemet. Benytt prosessen for *Verdivurdering av informasjon*.

Linker

Prosess - Verdivurdering av informasjon

Sjekk om system faller inn under sikkerhetsloven

Prosesseier: Ole Jakob Ottestad | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 9.2.2024 | Publisert versjon: 1

Inngang:

Verdivurdering av informasjonen som behandles eller objektet som IT systemet opererer på er utført og dokumentert.

Omfang/Aktiviteter:

Gjennomgang av verdiene som er dokumentert i forrige steg.

Sjekk spesielt mot Lov om nasjonal sikkerhet (SIK) §6.

Klargjør om det er behov for godkjenning av skjermingsverdig informasjonssystem og hvem som eventuelt må godkjenne systemet før innføring. (SIK §6-3 og VSF§50/§51)

Resultat

Avklart behov for godkjenning av skjermingsverdig informasjonssystem og hvilken godkjenningsmyndighet som gjelder.

Dokumentert informasjon (styrende dokumentasjon)

Prosedyre

Prosedyre for å dokumentere sikkerhetskrav til skjermingsverdig informasjonssystem

Risikovurdering

Prosesseier: Ole Jakob Ottestad | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 9.2.2024 | Publisert versjon: 1

Gjennomfør en risikovurdering fokusert på informasjonssikkerhet. Målet er å avdekke hvilke tiltak som er nødvendig for å oppnå et akseptabelt sikkerhetsnivå ved innføringen av IT løsningen.

Linker

Prosess - Risikovurdering

Fastsette nødvendige tiltak

Prosesseier: Ole Jakob Ottestad | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 9.2.2024 | Publisert versjon: 1

Inngang:

Risikovurdering med fokus på informasjonssikkerhet og personvern er gjennomført.

Omfang/Aktiviteter:

Foreslåtte tiltak gjennomgås og besluttes.

Tiltak flyttes til design og klargjøres for implementering.

Merk at tiltak kan omfatte både tekniske, prosessmessige og organisatoriske elementer.

Merk at i de tilfellene at det er nasjonal myndig som skal godkjenne skjermingsverdig informasjonssystem så må systemet dokumenteres iht til de krav som stilles fra myndighetene. Referer til https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-for-godkjenning-av-informasjonssystem/

Det er viktig at alle tiltak vurderes mot «Delstrategi IT» for å sikre at tiltak faller innenfor de interne kravene til NND. Dersom tiltak medfører brudd på interne regler, eller nødvendige tiltak ikke er praktisk mulig å gjennomføre, så må dette behandles i delprosessen «IT arkitekturstyring»

Resultat:

Systemdokumentasjon oppdateres med design. Det legges sporing tilbake til vedtatte tiltak og risikovurderingen. Eventuelle endringer i prosesser eller organisatoriske elementer er identifisert og klargjort for endring.

Dokumentert informasjon (styrende dokumentasjon)

Prosedyre

Prosedyre for å dokumentere sikkerhetskrav til skjermingsverdig informasjonssystem

Iverksette tiltak

Prosesseier: Ole Jakob Ottestad | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 9.2.2024 | Publisert versjon: 1

Inngang:

Design er utført og klargjort for implementering

Omfang/Aktiviteter:

De avtalte tiltakene implementeres i systemet, prosesser og organisasjon.

Aktivitetene skal utføres i samsvar med beskrivelsene i delprosessen «Håndtere IT endring».

Resultat:

IT systemet er klar til validering mot avtalte tiltak.

Validere at tiltakene virker

Prosesseier: Ole Jakob Ottestad | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 9.2.2024 | Publisert versjon: 1

Inngang:
IT systemet er klar for validering av avtalte tiltak.

Omfang/Aktiviteter:
Alle tiltak valideres gjennom avtalte prosedyrer. Validering kan skje med en kombinasjon av testing, inspeksjoner eller andre metoder.
Det skal utarbeides skriftlig dokumentasjon på hvordan de ulike tiltakene skal valideres, hvilke data som skal benyttes for valideringen og hva som er forventet resultat av valideringen i forkant av gjennomføring av valideringen.
Være spesielt oppmerksom på kravene i SIK §6-5 og SIK §6-6 når det kommer til test av tekniske tiltak.
Validering skal utføres i samsvar med beskrivelsene i delprosessen «Testing og verifikasjon».

Resultat:
Avtalte tiltak er validert og resultatet av valideringen er dokumentert i egen.

Skaff eventuell godkjenning

Prosesseier: Ole Jakob Ottestad | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 9.2.2024 | Publisert versjon: 1

Inngang:

Alle identifiserte tiltak er implementert og validert

Omfang/Aktiviteter:

For de systemene som er søknadspliktige iht SIK og VSF så utarbeides formell søknad om godkjenning og sendes til godkjennende myndighet.

Resultat:

Godkjenning innhentet til å ta i bruk IT systemet.

Dokumentert informasjon (styrende dokumentasjon)

Prosedyre

Prosedyre for å dokumentere sikkerhetskrav til skjermingsverdig informasjonssystem

Veiledning

Brukerveiledning dokumentasjon av gradert informasjonssystem

Ta informasjons- systemet i bruk

Prosesseier: Ole Jakob Ottestad | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 9.2.2024 | Publisert versjon: 1

Inngang:

Alle godkjenninger er mottatt

Omfang/Aktiviteter:

NND gjennomfører nødvending opplæring/innføring, gjennomfører utrulling og tar IT systemet i bruk.

Aktivitetene for utrulling skal skje i henhold til beskrivelsene i delprosess «Håndtere utrulling»

Resultat:

Godkjent IT system er tatt i bruk av NND.