7 Forvaltning (drift)

Sjekklisten er dynamisk, ikke uttømmende og skal oppdateres regelmessig. Dersom du har innspill til noen av punktene, vil vi gjerne høre fra deg.

Hvordan håndtere hendelser og avvik?

- Etabler og utøv plan for hendelseshåndtering (gjort i produksjonssetting) i virksomhetens plan for hendelseshåndtering.
- Sikkerhetshendelser gis høy prioritet.
- Håndter hendelser og avvik:
  - **Detekter** unormal og avvikende aktivitet, trafikk, sikkerhetshendelser og avvik.
  - **Verifiser** om unormal og avvikende aktivitet, trafikk, sikkerhetshendelser og avvik er et faktisk sikkerhetsbrudd eller falsk positiv.
  - **Rapporter** sikkerhetsbrudd og avvik slik interne retningslinjer for hendelseshåndtering tilsier.
  - **Håndter** sikkerhetshendelser og avvik i henhold til virksomhetens kontinuitetsplan for å gjenopprette **normaltilstand** for forvaltning, drift og vedlikehold.
- Øv regelmessig på uventede scenarier.

Forvaltning, drift og vedlikehold

- Identifiser og fordel roller, ansvar og myndighet.
- Håndter de registrertes rettigheter og forespørsler knyttet til dette, for eksempel om innsyn, endring, sletting, dataportabilitet, samtykke, informasjon, åpenhet med mer.
- Vurder kontinuerlig effekten av tekniske og organisatoriske sikkerhetstiltak for avdekke sårbarheter.

  Eksempler:
  - sikkerhetstester (slik som sårbarhetsanalyser og penetrasjonstester, fortløpende automatisk helsesjekk av applikasjon og infrastruktur)
  - øvelser (slik som emne- og bransjeøvelser, desktop, spill med mer)
  - testing og måling av sikkerhetskultur (slik som kampanjer, tester som må besvares)

- Mål effekten av sikkerhetstiltak i henhold til hensikt.
- Forvaltning av data, plattform, nett og programvare omfatter
  - å identifisere mulige angrepspunkter. Overvåk disse punktene, for eksempel applikasjoner, server, nettverk, endepunkt med mer
  - feilretting, oppdatering og patching av server- eller klientprogramvare og tredjepartskomponenter
  - ytelsesforbedringer
  - logging av system- og brukeraktivitet for sikkerhetssjekk
  - regelmessig gjennomgang av logger for å avdekke sikkerhetsavvik
  - retting, sletting og utfasing av data og program, for eksempel utviklere som har oversikt over hele produksjonsprosessen og som fortløpende gjør tiltak for å forbedre driftsløsning
  - oppgraderinger og utfasing av programvarebibliotek
  - ivaretagelse nye sikkerhetsutfordringer og håndtere nye sårbarheter
  - oppdatering og forvaltning av kryptoalgoritmer og nøkler

- Følg NSMs tiltak mot dataangrep (https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-02-ti-viktige-tiltak-mot-dataangrep.pdf).
- Oppdater beredskap- og kontinuitetsplaner.
- Gjennomfør regelmessig øvelser på planverket.
- Gjennomfør regelmessig revidering og egenkontroll for å dokumentere samsvar med regelverk, og lukk avvik.
- Revider databehandlere mot databehandleravtalen og relevante revisjonskriterier regelmessig, for eksempel lovverk, adferdsnormer (bransjenormer), interne bestemmelser, sikkerhetsrammeverk.
- Kontroller og gjennomgå bruker- og leverandørtilganger regelmessig.
- Utfør regelmessige risiko- og sårbarhetsanalyser basert på tidligere risiko- og sårbarhetsanalyser.
- Vurder personvernkonsekvenser ved vesentlig endringer eller utvikling av programvare.
- Etabler og presenter status vedrørende personvern og sikkerhet for ledelsen.

Hvorfor stille krav til forvaltning, drift og vedlikehold?

- Behandlingsansvarlig skal ha oversikt over behandlingsaktiviteter knyttet til personopplysninger og databehandlere skal ha tilsvarende oversikt over det de gjør på vegne av ulike behandlingsansvarlige, jf. artikkel 30.
- Det stilles krav til sikkerhet ved behandling av personopplysninger, jf. artikkel 32.
- Det stilles krav om innebygd personvern i løsninger, programmer, apper og system som forvalter personopplysninger, jf. artikkel 25.
- Det stilles krav om vurdering av personvernkonsekvenser ved oppstart eller vesentlige endring relatert til behandling av personopplysninger, jf. artikkel 35.
- Det stilles krav om å ivareta den registrertes rettigheter, jf. artikkel 12-23.
- Det stilles krav om å ivareta personvernprinsippene, jf. artikkel 5.
- Sikker forvaltning, drift og vedlikehold er forankret i virksomhetens ledelse.
- Det stilles krav til at behandlingsansvarlig skal benytte seg av databehandlere som er forpliktet til personvernforordningen, jf. artikkel 28.