Leverandøroppfølging – eksempler på sikkerhetsrelevant rapportering (faktaark 12)

Versjon 3.0

02. juni 2022

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket gir veiledning om hva som bør inkluderes i rapportering av sikkerhetsmessig betydning ved oppfølging av leverandører. Faktarket inneholder eksempler på informasjon og indikatorer som kan inngå i rapportering fra leverandør til kunde (virksomheter i helse- og omsorgssektoren) ved ulike typer leveranser. Formålet med faktaarket er å bidra til at virksomhetene i sektoren får rapportert sikkerhetsrelevant informasjon fra sine leverandører slik at nødvendige tiltak kan iverksettes
Målgruppe	Målgruppen for faktaarket er virksomheter som behandler helse- og personopplysninger og deres leverandører
Krav i Normen	Faktaarket gjelder for følgende kapitler i Normen - Kapittel 5.7 Leverandørforhold og avtaler - Kapittel 5.8 Håndtering av informasjonssikkerhetsbrudd
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: - Personvernforordningen artikkel 32 Sikkerhet ved behandlingen, bokstav d - Personvernforordningen artikkel 33 Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten - Veileder for fjernaksess mellom virksomhet og leverandør - NSM grunnprinisipper for IKT-sikkerhet: 2.1.9 - NSM grunnprinisipper for IKT-sikkerhet: 2.1.10 -

Tilbakerapportering av resultater fra IKT-driften

Leverandører til helse- og omsorgssektoren skal tilrettelegge for at dataansvarlig som tar i bruk leverandørens produkter og tjenester, kan oppfylle lovbestemte krav og krav i Normen. Den dataansvarlige har ansvaret for at krav til informasjonssikkerhet og personvern følges gjennom hele leveransekjeden. I leveranser av f.eks. tjenester, maskinvare eller systemer skal det avtales skriftlig med leverandører hvilke sikkerhetskrav som skal oppfylles for at den dataansvarlige skal kunne oppfylle sitt ansvar.

Avtalen bl.a. bør innholde krav til sikkerhetsrelevant rapportering fra leverandør til kunde. Faktaarket innholder eksempler på hva som kan inngå i slik rapportering.

Informasjonssikkerhet og personvern knyttet til anskaffelser og leverandøroppfølging skal inngå i virksomhetens styringssystem for informasjonssikkerhet. Alle faser i leverandørstyring, fra anskaffelse til avtalen er avsluttet, skal omfattes.

Avgrensning

Faktaarket gir ikke utfyllende detaljer om rapportering fra underleverandører, eller andre aspekter ved leverandøroppfølging og anskaffelser.

Kompletterende veiledningsmateriell

NSM grunnsprinsipper for IKT-sikkerhet: 2.1.9 og 2.1.10

NSM: Sikkerhetsfaglige anbefalinger ved tjenesteutsetting

Direktoratet for e-helse: Informasjonssikkerhet ved bruk av private leverandører

1	**Driftsstatus på kritiske system** Generell driftsstatus på kritiske IKT-system, for eksempel elektronisk pasientjournalsystem (EPJ) bør jevnlig rapporteres til virksomhetens ledelse. Eksempel på parametere som kan inngå i rapportering: – Oppetid på systemer – Planlagte avbrudd og tidslengde på avbrudd – Feilsituasjoner som ikke blir definert som avvik – Mislykkede påloggінger, glemte passord etc. – Feilsituasjoner som fremkommer i hendelsesregistre – Utvikling og trender for indikatorer og nøkkeltall
2	**Oppfølging av avviksrapportering** Alvorlige feil og hendelser skal rapporters som avvik. Spesielt bør dette gjøres når det er avdekket avvik fra vedtatte prosedyrer og nivå for akseptabel risiko. Oppfølging og status på avviksrapportering bør rapporteres jevnlig som en del av resultatene fra driften. Oppfølgingen bør omfatte både avvik og andre forhold som blir rapportert.For mer informasjon se veileder om internkontroll for informasjonssikkerhet og personvern..

3	**Meldingskommunikasjon (EDI)** Status på meldingskommunikasjonen sier noe om hvordan virksomheten ivaretar elektronisk samhandling med andre (for eksempel henvisning, epikrise, resepter, behandlerkrav, laboratoriesvar, SMS, applikasjonskvittering, osv). Gode prosedyrer rundt elektronisk samhandling er viktig for å ivareta tilfredsstillende informasjonssikkerhet. Parametere som kan inngå i rapportering er for eksempel – Meldinger uten kvittering – Ikke-planlagte stans i meldingskommunikasjon – Planlagte stans i meldingskommunikasjon – Feilsendte meldinger (for eksempel meldinger med feil mottaker og -adresse) – Meldinger med negativ applikasjonskvittering – antall og feiltype
4	**Systemleverandør** Rapportering fra systemleverandører (for eksempel for EPJ) er viktig med tanke på ha stabil og god drift av viktige systemer. Rapporteringer bør foregå jevnlig og inneholde viktig informasjon i forhold til informasjonssikkerhet. Eksempel på parametere som kan inngå i rapportering: – Planlagte endringer, forventet effekt og tidspunkt de skal utføres – Sikkerhetsoppdateringer (med angivelse av resultat) – Feilrettinger – Systemoppdateringer (med angivelse av resultat)
5	**Databehandler** Databehandler skal iht databehandleravtalen jevnlig gi statusrapporter om resultater fra sine ansvarsområder tilbake til dataansvarlig (som vanligvis er virksomhetens ledelse). Det presiseres at en databehandler er en ekstern person/virksomhet utenfor den dataansvarliges virksomhet. Eksempel på parametere som kan inngå i rapportering: – Planlagte endringer, forventet effekt og tidspunkt de skal utføres – Feilsituasjoner – Konfigurasjonsendringer – Oppetid – Feilsituasjoner som fremkommer i hendelsesregistre – Manglende oppfyllelse av SLA (servicenivåavtale) og mulig årsaker
6	**Nettleverandører (for eksempel Norsk Helsenett)** Nettleverandøren er som regel ansvarlig for at kommunikasjonskanalen er tilgjengelig og sørger for transport av kommunikasjon over nettet. At nettet fungerer som det skal er en viktig forutsetning for å kunne etablere sikker elektronisk kommunikasjon. Eksempel på parametere som kan inngå i rapportering: – Feilsituasjoner, nedetid – Endringer i nettet som kan gi konsekvenser for virksomheten – Manglende oppfyllelse av SLA (servicenivåavtale) og mulig årsaker

7	**Ondsinnet programvare** Ondsinnet programvare kan være en reell trussel mot informasjonssikkerheten og kan komme for eksempel gjennom e-post, minnepinne eller ved nedlasting av data fra andre nett. Eksempel på parametere som kan inngå i rapportering: – Hendelser som har medført konsekvenser for virksomheten – Hvilke tiltak som er iverksatt og resultater av disse – Forslag til eventuelle forebyggende tiltak
8	**Status for sikkerhetsbarriere (for eksempel brannmur)** Trafikk som slipper gjennom sikkerhetsbarrierer kan være ondsinnede angrep som prøver å få tilgang til virksomhetens datanettverk. Sikkerhetsbarrierer krever jevnlige oppdateringer og konfigurasjonsendringer. Eksempel på parametere som kan inngå i rapportering: – Hendelser som har medført konsekvenser for virksomheten – Hvilke tiltak som er iverksatt og resultater av disse – Forslag til eventuelle forebyggende tiltak