Sikkerhetsrevisjon iflg. faktaark nr. 6 fra Norm for informasjonssikkerhet

Nr	Sjekkpunkt	Faktaark	Ok/ikke ok	Beskrivelse
1	Er det gjennomført nødvendig(e) risikovurdering(er) siste år?	7	Ok	Er gjennomført ROS-analyser for Sectra, DipsLab, Labcraft, Partus, AMIS og RBO 113. Dips og MTU gjenstår.
2	Er prosedyrene for avviksbehandling ift. informasjonssikkerhet kjent i virksomheten?	8	Ok	13 meldte info.sikk.avvik i 2016. En nedgang fra 19 fra 2015. 7 meldte avvik så langt i 2017.
3	Fungerer avviksbehandling ift. informasjonssikkerhet?	8	Ok	De ansatte har nok fortsatt for høy terskel før de melder informasjonssikkerhets avvik.
4	Er det etablert nødprosedyrer ved stans i informasjonssystemene?	11 HN-IKT	Ok	Nødprosedyrer for DIPS er etablert. Fra teknisk side (HN-IKT) foreligger det rutiner for håndtering av krisesituasjoner, i tillegg til vaktordninger 24/7. Ved linjebrudd har vi også nå redundante linjer (doble linjer)
5	Gjennomføres det jevnlig kontroll/gjennomgang av hendelsesregistre?	15	Ikke ok	Skal gjennomføres 4 innsynskontroller årlig, har i 2017 manglet loggkontrollører ved alle 3 enheter.
6	Krypteres helse- og personopplysninger (f.eks. meldingsformidling) som overføres i åpne nett?	16 og 24 HN-IKT	Ok	Når det gjelder den delen som faller under Faktaark 24, så krypteres all trafikk mellom sykehusene på nettverksnivå.
7	Er det etablert tilfredsstillende fysisk sikring av områder og datautstyr?	17 HN-IKT	Ok	Dette blir i økende grad bedre for hvert år. Nytt datasenter i Tromsø er oppe og går og ROS-analyser er gjennomført her.
8	Er lagringsenhet på bærbart utstyr som benyttes til helse- og personopplysinger kryptert?	18 HN-IKT	Ok	Etter gjeldende prosedyrer er ikke personopplysninger tilgjengelig for lagring på bærbart utstyr. Bærbare datamaskiner som brukes ute på Internett, er gjennom konfigurering ikke godkjent for tilkopling inn på lokalnett for direkte tilgang til tjenester med sensitive personopplysninger.

Nr	Sjekkpunkt	Faktaark	Ok/ikke ok	Beskrivelse
9	Oppdateres antivirusprogramvaren kontinuerlig?	19 HN-IKT	Ok	Ja, antivirusprogramvaren oppdateres hver time. HN IKT jobber fortløpende med å sikre utstyr som de er ansvarlig for.
10	Tas det daglig sikkerhetskopi?	21 HN-IKT	Ok	Ja, backup tas på alle 3 sykehus enhetene.
11	Oppbevares sikkerhetskopier utenfor huset?	21 HN-IKT	Ok	Ja. Sykehusene har Gb samband og backup skjer til Bodø eller Tromsø der de har backup roboter. Alt av backup går dit. HN-IKT har i driftsavtale med oss ansvar for backup.
12	Er det kontroll med all ekstern tilgang til datasystemer?	22 HN-IKT	Ok	Ekstern tilgang skal være i samsvar med etablerte prosedyrer. Egen ROS-analyse vil bli gjennomført i løpet av året.
13	Følges ”Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet” ved eventuell ekstern tilgang?	36 HN-IKT	Ok	Samme svar som til pkt.12
14	Er det etablert relevante avtaler for forskningsprosjekter?	23	Ok	Ja
15	Slettes helse- og personopplysinger når formålet med behandlingen er avsluttet?	25 HN-IKT	Ok	Vedr. Pasopp undersøkelsene blir alt slettet når det skal, her må dedikerte HN-IKT personell svare på om det er gjort.
16	Brukes trådløst utstyr og nett iht. etablerte prosedyrer?	26 HN-IKT	Ok	Trådløse gjestenett er etablert via ikt-bestiller og av enhetene sjøl.
17	Etterleves prosedyrene for makulering?	27	Ok	I henhold til resultatene fra gjennomførte ROS-analyser etterleves prosedyrene.
18	Etterleves prosedyrene for bruk av e-post og Internett?	27 og 33	Ok	I henhold til resultatene fra gjennomførte ROS-analyser etterleves prosedyrene.
19	Etterleves prosedyrene for hjemmekontor og mobilt utstyr?	29 og 30 HN-IKT	Ok	Ny portal løsning er under implementering, verifisering av brukerne vil da skje.

Nr	Sjekkpunkt	Faktaark	Ok/ikke ok	Beskrivelse
20	Er det etablert løsning og prosedyrer for autentisering på sikkerhetsnivå 4 ved bruk av mobiltelefoner og nettbrett for tilgang til helseopplysninger?	30 HN-IKT	Ikke ok	Ny portal løsning skal ha sikkerhetsnivå 3, lokale sertifikater (Nivå 3) i kort er ikke implementert enda men det kommer i løpet av noen måneder.
21	Byttes passord iht. prosedyrene?	31	Ok	Ja. Synkronisering av brukernavn/passord fra flere systemer er allerede etablert og flere vil komme i 2017.
22	Følges veileder ”Personvern og informasjonssikkerhet i forskningsprosjekter innefor helse- og omsorgssektoren” ifm utlevering av helse- og personopplysninger?	40	Ok	I de aktuelle forskningsprosjektene gjøres det.
23	Etterleves reglene for bruk av SMS i pasientkontakt?	42	Ok	Er SMS pilot i Dips for ei avd. ved Psyk helse og rus for påminnelse av time.
24	Etterleves reglene for bruk av testdata i systemer som inneholder helse- og personopplysninger?	43 HN-IKT	ok	Er ikke kjent med at det ikke etterleves. Lederne skal forhøre seg litt.

Pkt.'er som ikke er ok:

Nr	Sjekkpunkt	Faktaark	Ok/ikke ok	Beskrivelse
5	Gjennomføres det jevnlig kontroll/gjennomgang av hendelsesregistre?	15	Ikke ok	Skal gjennomføres 4 innsynskontroller årlig, har i 2017 manglet loggkontrollører ved alle 3 enheter.
20	Er det etablert løsning og prosedyrer for autentisering på sikkerhetsnivå 4 ved bruk av mobiltelefoner og nettbrett for tilgang til helseopplysninger?	30 HN-IKT	Ikke ok	Ny portal løsning skal ha sikkerhetsnivå 3, lokale sertifikater (Nivå 3) i kort er ikke implementert enda men det kommer i løpet av noen måneder.

Tiltak:

Punkt	Innhold	Tiltak
5	Gjennomføres det jevnlig kontroll/gjennomgang av hendelsesregistre?	Loggkontrollørene ved alle 3 enheter er pensjonister nå, enhetene har fått varsel om å utpeke ny loggkontrollør. Forventet å kunne gjenoppta loggkontrollene i løpet av høsten 2017.
20	Er det etablert løsning og prosedyrer for autentisering på sikkerhetsnivå 4 ved bruk av mobiltelefoner og nettbrett for tilgang til helseopplysninger?	Info.sikk ansvarlig følger opp HN-IKT i deres implementering av Nivå 3 løsning, den skal etter plan være operativ tidlig høst 2017.

Tiltakene iverksettes.

Dato: 13.06.2017
Sign: adm. direktør

_____