European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

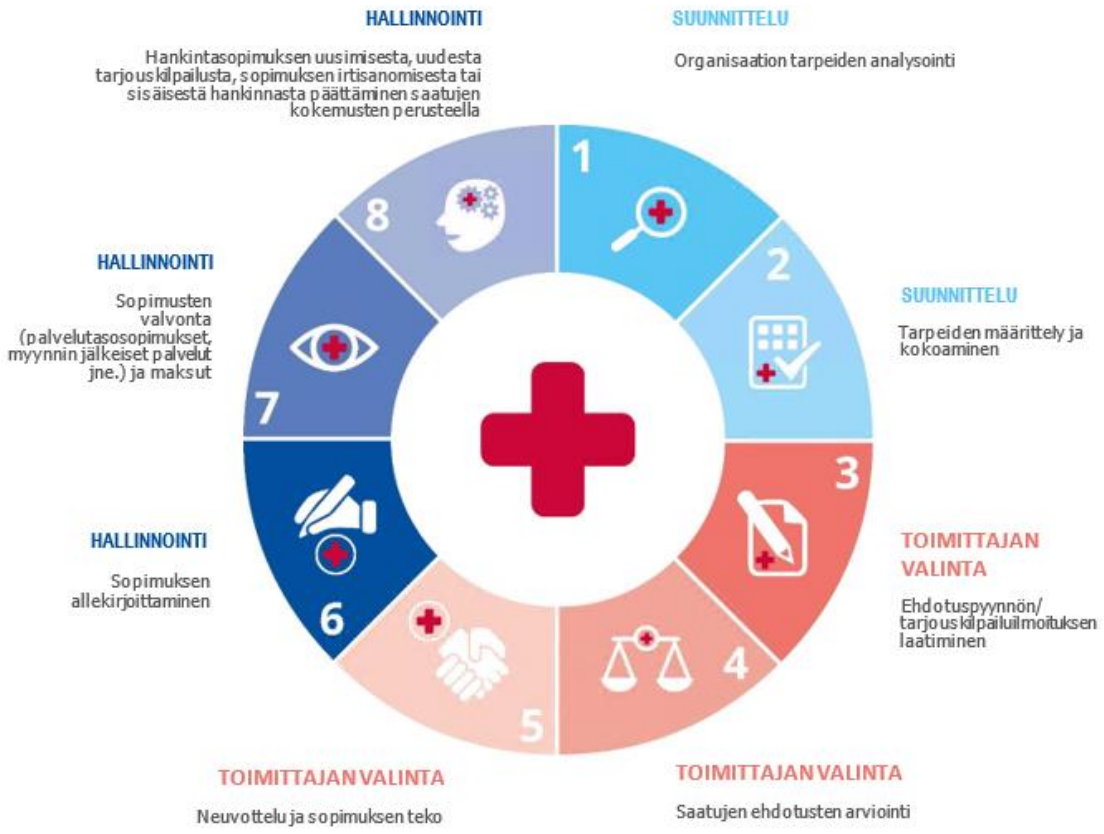
SAIRAALOIDEN HANKINTOJA KOSKEVAT KYBERTURVALLISUUSOHJEET

Raportin tarkoitus on toimia eräänlaisena ohjekirjana terveydenhuollon ammattilaisille. Monet käytännöt ja suositukset ovat hyödyksi myös muille terveydenhuollon organisaatioille, koska hankintamenettelyt voivat olla varsin samankaltaisia. Ohjeista on hyötyä sairaaloiden teknisiä tehtäviä hoitaville terveydenhuollon ammattilaisille, toisin sanoen organisaation johtotason työntekijöille, joita ovat terveydenhuollon organisaatioiden tietojärjestelmien turvallisuusvastaavat, teknologiajohtajat, tietohallintotiimien jäsenet sekä hankintavastaavat. Tässä lyhyessä asiakirjassa käsitellään raportin keskeisiä seikkoja. Yksityiskohtaisia tietoja saa helmikuussa 2020 julkaistusta ENISAn asiakirjasta ENISA Good Practices for the Security of Healthcare Services

HANKINTAMENETTELY

Koska sairaalan ekosysteemi koostuu useista tietoteknisistä komponenteista, kyberturvallisuutta olisi tutkittava erikseen kaikissa näissä komponenteissa. Kyberturvallisuuden olisi oltava osana hankintamenettelyn kaikkia eri vaiheita. Tässä osiossa esitellään yhteisiä vaiheita tuotteiden ja palvelujen, kuten lääkinnällisten laitteiden, tietojärjestelmien ja infrastruktuurien, hankintamenettelyissä.

Kuva 1: Hankintamenettelyn elinkaari sairaaloissa



- Suunnitteluvaihe: Aluksi sairaala tutkii, mitkä sen tarpeet ovat, ja kerää tietoa tarpeista useilta osastoilta organisaation sisällä. Jos esimerkiksi hankitaan uusi pilvipalvelu, teknologiajohtajan olisi määriteltävä tarpeet ja oltava selvillä siitä, millä tavoin kyseistä palvelua voidaan hyödyntää.

- Toimittajan valinta: Tämän jälkeen tarpeiden pohjalta tehdään tekniset eritelmät ja aloitetaan hankintaprosessi yhteistyössä hankintaosaston kanssa (esim. julkaisemalla tarjouskilpailuilmoitus). Sairaala vastaanottaa vaatimusten mukaiset tarjoukset, minkä jälkeen toimikunta (johon kuuluu teknologiajohtaja / tietojärjestelmien turvallisuusvastaava ja/tai yksi tietohallintotiimin jäsen) arvioi tarjoukset ja valitsee parhaiten soveltuvat tuotteet. Toimeksisaajan kanssa käydään neuvotteluja ja tehdään hankintasopimus.

- Hallinnointivaihe: Lopuksi hankintasopimus (hallinnointi ja seuranta) annetaan hallinnoinnista vastaavan työntekijän (business owner) hoidettavaksi. Tehtävän saanut henkilö päättää tarjouskilpailun ja ottaa vastaan käyttäjien palautteet laitteen/järjestelmän/palvelun käytännön toimivuudesta.

SAIRAALAHANKINTOJEN TYYPIT

Taulukko 1: Hankintojen tyypit (käyttöomaisuuden luokittelu)

Hankinnan tyyppi	Tyypin kuvaus
Kliiniset tietojärjestelmät	Käsittää kaikentyyppisten sairaanhoitoon liittyvien ohjelmistojen hankinnan
Lääkinnälliset laitteet	Kaikki sairauksien hoitoon, torjuntaan tai diagnosointiin tarkoitetut laitteet
Verkkolaitteet	Verkkojohdot (koaksiaali- ja valokaapelit), yhdyskäytävät, reitittimet, kytkimet, palomuurit, virtuaaliset yksityisverkot, tunkeutumisenestojärjestelmät, tietomurtohälyttimet jne.
Etähoitojärjestelmät	Varusteet tai laitteet sairaalaympäristön ulkopuolella annettavaa hoitoa varten, etenkin kotisairaalahoitoa varten
Asiakkaiden mobiililaitteet	Kaikki ohjelmat, joiden avulla annetaan terveydenhoidollista apua tai kerätään lääketieteellistä tietoa ja joita ei ole liitetty suoraan sairaalan verkkoon; esimerkiksi terveydenhuollon etäpalvelusovellukset
Tunnistusjärjestelmät	Järjestelmät, joiden avulla potilaat tai lääketieteellinen henkilökunta voidaan tunnistaa yksilöllisesti (biometriset skannerit, kortinlukijat jne.) ja joilla varmistetaan käyttäjien tunnistaminen ja/tai oikeus käyttää tietojärjestelmiä
Kiinteistöjen hallinnointijärjestelmät	Kaikentyyppiset rakennelmat ja rakennukset, joissa voi olla lääkintätiloja
Keskusvalvontajärjestelmät	Keskusten kaikkia fyysisiä osatekijöitä valvovat järjestelmät, kuten energiansäätöjärjestelmät, ovien lukitusjärjestelmät ja kameravalvontajärjestelmät
Ammatilliset palvelut	Kaikentyyppiset ammattihenkilöiden tai yritysten tarjoamat ulkoistetut tai ulkoistamattomat palvelut, kuten terveydenhuolto-, kuljetus- ja kirjanpitopalvelut sekä tekniset palvelut ja tietotekniikka-, oikeudelliset, huolto-, siivous- ja ateriapalvelut jne.
Pilvipalvelut	Kaikki viestintä- ja tietojärjestelmät tai muut tietojärjestelmät, jotka eivät ole sairaalarakennuksessa eivätkä datakeskuksen tiloissa sairaalan tietotekniikkaosaston asianmukaisessa valvonnassa

UHKALUOKITTELU

Erityyppisiin hankintoihin liittyy erilaisia uhkia sairaalan tieto- ja viestintätekniselle toimintaympäristölle. Tutustukaa tässä osiossa esitettyyn uhkaluokitteluun yhdessä organisaation tietotekniikka-, turvallisuus- tai riskiosaston kanssa ja selvittäkää, mitkä uhat ovat organisaation kannalta merkittävimmät. Luokitteluun olisi hyvä tutustua osana sairaalan tietotekniikkaan liittyviä tehtävänkuvia hankintapotentiaalista riippumatta.

Taulukko 2: Uhkatyypit (Uhkaluokittelu)

Uhka	Esimerkkejä
Luonnonilmiöt	Tulipalot, tulvat tai maanjäristykset
Häiriö toimitusketjussa	Pilvipalvelun tarjoajaan tai verkkopalvelun tarjoajaan liittyvä häiriö, sähkökatkos, lääkinnällisten laitteiden valmistajan virhe / vapautus vastuusta
Inhimilliset virheet	Lääkintäjärjestelmän konfiguraatiovirhe, jäljityslokien tai luvattoman pääsyn valvonnan puuttuminen / prosessien puuttuminen, vaatimustenvastaisuus (työntekijöiden omien laitteiden käyttö), lääkintähenkilökunnan / potilaan virhe
Ilkivalta	Haittaohjelmat (virukset, kiristyshaittaohjelmat, työntekijöiden omien laitteiden käyttö työtehtävissä (BYOD), kaappaukset (kryptokaappaus, lääkinnällisten laitteiden kaappaus), käyttäjän manipulointi (verkkourkinta, palkinnoilla houkuttelu, laitteiden kloonaus), varkaus (tietojen tai laitteiden), lääkinnällisten laitteiden peukalointi, salakopiointi, palvelunesto, verkkohyökkäykset, verkkosovellushyökkäykset, sisäpiiriuhat, fyysinen manipulointi / vahingoittaminen, identiteettivarkaus, kybervakoilu, komponenttien mekaaninen tuhoaminen
Järjestelmäviat	Ohjelmistoviat, vanhentuneet laiteohjelmistot, laiteviat, verkkokomponenttien toimintahäiriöt, puutteellinen huolto

HANKINTOJEN KYBERTURVALLISUUTTA KOSKEVAT HYVÄT KÄYTÄNNÖT

Alla oleva hyvien käytäntöjen luettelo ei ole tyhjentävä. Siitä on kuitenkin konkreettista hyötyä sairaalan laitehankinnoista vastaaville terveydenhuoltoalan tietotekniikka-ammattilaisille. Hyvät käytännöt on laadittu terveydenhuollon ammattilaisten haastatteluista saatujen tietojen perusteella Lukija voi mukauttaa luetteloa oman organisaationsa painopisteiden mukaan.

Käytäntö 1. Tietotekniikkaosasto otetaan mukaan hankinnan eri vaiheisiin. Näin varmistetaan, että kyberturvallisuusnäkökohtia koskeva asiantuntemus otetaan huomioon.

Hankinnan vaiheet: Kaikki

Asiaan liittyvät hankintatyypit: Kaikki

Asiaan liittyvät uhat: Kaikki

Käytäntö 2. Toteutetaan haavoittuvuuksien tunnistamis- ja hallintamenettely sen varmistamiseksi, että haavoittuvuudet otetaan huomioon ennen uusien tuotteiden ja palvelujen hankkimista ja että olemassa olevien tuotteiden ja palveluiden haavoittuvuuksia seurataan niiden koko elinkaaren ajan.

Hankinnan vaiheet: Kaikki

Asiaan liittyvät hankintatyypit: Kliiniset tietojärjestelmät, lääkinnälliset laitteet, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Kaikki

Käytäntö 3. Laaditaan laitteistojen ja ohjelmistojen päivittämistä koskevat toimintaperiaatteet, joilla varmistetaan, että käyttöjärjestelmän ja ohjelmistojen uusimpia päivityksiä käytetään ja että virustorjuntaohjelmaa päivitetään.

Hankinnan vaiheet: Kaikki

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kliiniset tietojärjestelmät, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat

Käytäntö 4. Parannetaan langattoman viestinnän turvallisuuden valvontaa sen varmistamiseksi, että pääsy sairaalan Wi-Fi-verkkoon on rajoitettu ja sitä valvotaan tiukasti.

Hankinnan vaiheet: Kaikki

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, etäasiakaslaitteet, tunnistusjärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, inhimilliset virheet

Käytäntö 5. Laaditaan testauksen toimintaperiaatteet, joilla varmistetaan, että hiljattain hankitulle tai hiljattain konfiguroiduille tuotteille tehdään tunkeutumistesti ja että korjaavat toimet toteutetaan tosiasiallisen ympäristön toimintaparametrien mukaisesti.

Hankinnan vaiheet: Kaikki

Asiaan liittyvät hankintatyypit: Kliiniset tietojärjestelmät, lääkinnälliset laitteet, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, kiinteistöjen hallinnointijärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, järjestelmäviat, inhimilliset virheet

Käytäntö 6. Laaditaan toiminnan jatkuvuussuunnitelmia sen varmistamiseksi, että järjestelmän toimintahäiriö ei keskeytä sairaalan keskeisiä palveluja ja että järjestelmätoimittajan rooli on määritelty tarkasti.

Hankinnan vaiheet: Kaikki

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kliiniset tietojärjestelmät, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat

Käytäntö 7. Otetaan huomioon yhteentoimivuusongelmat ja varmistetaan, että olemassa olevissa komponenteissa (aiemmassa tietotekniikassa) ei ole turvallisuuspuutteita.

Hankinnan vaiheet: Kaikki

Asiaan liittyvät hankintatyypit: Kliiniset tietojärjestelmät, lääkinnälliset laitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Järjestelmäviat, inhimilliset virheet, ilkivalta

Käytäntö 8. Mahdollistetaan kaikkien komponenttien testaus, jolla varmistetaan, että ne täyttävät lupaukset: tarkastetaan käytön helppous, tutkitaan tulosten oikeellisuus kuormitettuna ja tutkitaan, onko tietoturvassa aukkoja (huonot salasanakäytännnöt, SQL-injektio).

Hankinnan vaiheet: Kaikki

Asiaan liittyvät hankintatyypit: Kliiniset tietojärjestelmät, lääkinnälliset laitteet, etäasiakaslaitteet, tunnistusjärjestelmät, pilvipalvelut, keskusvalvontajärjestelmät, etähoitojärjestelmä, kiinteistöjen hallinnointijärjestelmät, asiakkaiden mobiililaitteet

Asiaan liittyvät uhat: Ilkivalta, inhimilliset virheet, järjestelmäviat, häiriö toimitusketjussa

Käytäntö 9. Huolehditaan auditoinnista ja lokikirjanpidosta, jotta voidaan jäljittää hyökkääjät ja selvittää järjestelmän vaarantuessa, miten paljon tietoja on kadonnut/varastettu.

Hankinnan vaiheet: Kaikki

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat

Käytäntö 10. Salataan arkaluonteisia henkilötietoja tietojen siirron aikana ja muuna aikana määrittelemällä toimintaperiaatteet järjestelmille, palveluille ja laitteille, joilla käsitellään yleisen tietosuoja-asetuksen 9 artiklan mukaisia erityisiä henkilötietoryhmiä.

Hankinnan vaiheet: Kaikki

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kliiniset tietojärjestelmät, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat

Käytäntö 11. Tehdään riskinarviointi osana hankintamenettelyä.

Hankinnan vaiheet: Suunnittelu

Asiaan liittyvät hankintatyypit: Kaikki

Asiaan liittyvät uhat: Kaikki

Käytäntö 12. Suunnitellaan etukäteen verkkoa ja laitteistoa koskevat vaatimukset sekä lupavaatimukset, jotta voidaan määrittää, onko ennen asennusta tehtävä lisäparannuksia ja/tai -hankintoja uuden järjestelmän käyttöön ottamiseksi.

Hankinnan vaiheet: Suunnittelu

Asiaan liittyvät hankintatyypit: Kliiniset tietojärjestelmät, verkkolaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät

Asiaan liittyvät uhat: Häiriö toimitusketjussa, järjestelmäviat, luonnonilmiöt, inhimilliset virheet

Käytäntö 13. Tunnistetaan hankittaviin tuotteisiin tai palveluihin liittyvät uhat ja varmistetaan, että uhkien tunnistamista jatketaan hankinnan koko elinkaaren ajan.

Hankinnan vaiheet: Suunnittelu, hallinnointi

Asiaan liittyvät hankintatyypit: Kaikki

Asiaan liittyvät uhat: Kaikki

Käytäntö 14. Eriytetään organisaation verkko sen varmistamiseksi, että verkkoliikenne voidaan pitää erillään ja/tai sitä voidaan suodattaa. Näin voidaan rajoittaa pääsyä verkkovyöhykkeeltä toiselle tai estää se kokonaan.

Hankinnan vaiheet: Suunnittelu, hankintalähteen valinta

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kliiniset tietojärjestelmät, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat

Käytäntö 15. Määritetään verkkovaatimukset, jotta voidaan varmistaa yhteentoimivuus ja välttää puutteita verkon ja komponenttien topologian luomisen jälkeen.

Hankinnan vaiheet: Suunnittelu

Asiaan liittyvät hankintatyypit: Kliiniset tietojärjestelmät, verkkolaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut, etähoitojärjestelmät, asiakkaiden mobiililaitteet

Asiaan liittyvät uhat: Häiriö toimitusketjussa, järjestelmäviat, luonnonilmiöt

Käytäntö 16. Määritellään perustason tietoturvavaatimukset ja käytetään niitä hyväksyttävyyskriteereinä toimittajien valinnassa.

Hankinnan vaiheet: Suunnittelu, hankintalähteen valinta

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kliiniset tietojärjestelmät, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat

Käytäntö 17. Luodaan pilvipalvelujen hankintaa varten erityinen ehdotuspyyntö, jossa otetaan huomioon sääntelyyn liittyvät ja toimintapoliittiset vaatimukset.

Hankinnan vaiheet: Suunnittelu, hankintalähteen valinta

Asiaan liittyvät hankintatyypit: Pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa

Käytäntö 18. Annetaan etusija kyberturvallisuusjärjestelmien/-standardien mukaisesti sertifioidun käyttöomaisuuden hankinnalle.

Hankinnan vaiheet: Toimittajan valinta

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kliiniset tietojärjestelmät, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat

Käytäntö 19. Tehdään tietosuojaa koskevia vaikutustenarviointeja suunniteltaessa uuden järjestelmän tai palvelun hankintaa.

Hankinnan vaiheet: Toimittajan valinta

Asiaan liittyvät hankintatyypit: Kliiniset tietojärjestelmät, lääkinnälliset laitteet, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, ammatilliset palvelut, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, inhimilliset virheet

Käytäntö 20. Luodaan yhdyskäytäviä, jotka pitävät aiemmat järjestelmät/koneet yhdistettyinä ja tarjoavat näiden ryhmien välisten rajojen valvontaa, jos ryhmissä ilmenee ongelmia.

Hankinnan vaiheet: Toimittajan valinta, hallinnointi

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat

Käytäntö 21. Annetaan organisaation tietoturvakäytäntöjä koskevaa kyberturvallisuuskoulutusta sen varmistamiseksi, että organisaation omaa henkilöstöä tai organisaation tiloissa työskenteleviä ulkopuolisia alihankkijoita/konsultteja koulutetaan asianmukaisesti.

Hankinnan vaiheet: Toimittajan valinta, hallinnointi

Asiaan liittyvät hankintatyypit: Kaikki

Asiaan liittyvät uhat: Ilkivalta, inhimilliset virheet

Käytäntö 22. Laaditaan tietoturvapoikkeamien torjuntasuunnitelmia, jotka kattavat hiljattain hankitut tuotteet tai järjestelmät

Hankinnan vaiheet: Toimittajan valinta, hallinnointi

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kliiniset tietojärjestelmät, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat

Käytäntö 23. Otetaan myyjä/valmistaja mukaan tietoturvapoikkeamien hallintaan ja määritetään ehdotuspyynnössä asiaa koskevat selkeät ehdot.

Hankinnan vaiheet: Toimittajan valinta, hallinnointi

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kliiniset tietojärjestelmät, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat

Käytäntö 24. Suunnitellaan ja seurataan kaikkien laitteiden huoltotoimia, jotta voidaan varmistaa asianmukainen toimivuustaso ja päättää mahdollisista päivityksistä/korjauksista jne.

Hankinnan vaiheet: Toimittajan valinta, hallinnointi

Asiaan liittyvät hankintatyypit: Kliiniset tietojärjestelmät, verkkolaitteet, lääkinnälliset laitteet, kiinteistöjen hallinnointijärjestelmät, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Inhimilliset virheet, järjestelmäviat, luonnonilmiöt

Käytäntö 25. Etäkäyttö olisi minimoitava ja sitä olisi hallinnoitava siten, että ulkoinen viestintä toimittajan kanssa koskisi yksinomaan sen valvonnassa olevaa laitetta.

Hankinnan vaiheet: Toimittajan valinta, hallinnointi

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kliiniset tietojärjestelmät, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat, inhimilliset virheet

Käytäntö 26. Edellytetään korjauspäivityksiä kaikkiin komponentteihin ja sisällytetään tämä tieto ehdotuspyyntöön.

Hankinnan vaiheet: Toimittajan valinta, hallinnointi

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kliiniset tietojärjestelmät, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat

Käytäntö 27. Tiedotetaan henkilöstölle kyberturvallisuudesta sen varmistamiseksi, että henkilöstö on tietoinen hiljattain hankittuihin tuotteisiin tai palveluihin liittyvistä riskeistä.

Hankinnan vaiheet: Hallinnointi

Asiaan liittyvät hankintatyypit: Kaikki

Asiaan liittyvät uhat: Kaikki

Käytäntö 28. Toteutetaan käyttöomaisuuden inventointia ja konfiguraation hallintaa sen varmistamiseksi, että inventointia päivitetään asianmukaisesti, kun jokin komponentti lisätään tieto- ja viestintätekniikan toimintaympäristöön tai poistetaan sieltä, ja että tieto- ja viestintäteknisillä komponenteilla on perustason suojausasetukset ja niitä hallitaan asianmukaisesti.

Hankinnan vaiheet: Hallinnointi

Asiaan liittyvät hankintatyypit: Kliiniset tietojärjestelmät, lääkinnälliset laitteet, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät

Asiaan liittyvät uhat: Ilkivalta, inhimilliset virheet, järjestelmäviat

Käytäntö 29. Perustetaan erityiset pääsynvalvontajärjestelmät fyysisesti suojeltaviin tiloihin, joissa on lääkinnällisiä laitteita ja joihin olisi sallittava pääsy yksinomaan erikoistuneelle henkilöstölle.

Hankinnan vaiheet: Hallinnointi

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kiinteistöjen hallinnointijärjestelmät, tunnistusjärjestelmät

Asiaan liittyvät uhat: Ilkivalta, inhimilliset virheet

Käytäntö 30. Järjestetään usein toistuvia tai arkkitehtuurin/järjestelmän muuttamisen jälkeen tehtäviä tunkeutumistestejä ja sisällytetään niitä koskevat ehdot ehdotuspyyntöön.

Hankinnan vaiheet: Toimittajan valinta, hallinnointi

Asiaan liittyvät hankintatyypit: Lääkinnälliset laitteet, kliiniset tietojärjestelmät, verkkolaitteet, etähoitojärjestelmä, asiakkaiden mobiililaitteet, tunnistusjärjestelmät, keskusvalvontajärjestelmät, pilvipalvelut

Asiaan liittyvät uhat: Ilkivalta, häiriö toimitusketjussa, järjestelmäviat