STAKESIN TYÖPAPEREITA II / 2007

TYÖPAPEREITA

TERO TAMMISALO

Tietoturvakoulutuksen esitysmateriaali

Luennoitsijan muistiinpanot

STAKES

Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus

postimyynti: Stakes / Asiakaspalvelut PL 220, 00531 Helsinki
puhelin: (09) 3967 2190, (09) 3967 2308 (automaatti)
faksi: (09) 3967 2450 • Internet: www.stakes.fi

Taitto: Christine Strid

ISBN 978-951-33-1940-3 (nid.)
ISSN 1795-8091 (nid.)
ISBN 978-951-33-1941-0 (PDF)
ISSN 1795-8105 (PDF)

Stakes, Helsinki 2007

Valopaino Oy
Helsinki 2007

Tiivistelmä

Tero Tammisalo. Tietoturvakoulutuksen esitysmateriaali. Luennoitsijan muistiinpanot. Stakes, Työpapereita 11/2007. Helsinki 2007. 75 sivua, hinta 17 €. ISBN 978-951-33-1940-3

Tämä julkaisu sisältää tietoturvakouluttajan käyttöön tarkoitettua opetusmateriaalia. Julkaisussa ovat sosiaali- ja terveydenhuollon tietoturvan hallinnointioppaan sisältöön perustuvan koulutustarkoitukseen tehdyn esityksen muistiinpanot luennoitsijan työn tueksi ja muistiavuksi.

Julkaisua käytetään yhdessä koulutusdiasarjan kanssa. Diasarja on saatavissa Power Point -muodossa maksutta koulutuskäyttöön Stakesin sosiaali- ja terveysalan tietoyhteiskuntayksikön verkkosivulta osoitteesta http://sty.stakes.fi. Kouluttaja voi koota esityksensä käyttäen koulutusdioja valintansa mukaan. Esitykseen voi lisätä myös omia, esimerkiksi paikallista tilannetta kuvaavia, dioja. Stakesin dioja käytettäessä on lähteen oltava näkyvissä. Sosiaali- ja terveydenhuollon tietoturvan hallinnointiopas on myös saatavana Stakesin verkkosivuilta verkkojulkaisuna sekä tilattavissa painotuotteena.

Huomaa, että esitykseen on määritelty kaksi valmista esitystä: johto ja organisaatio. Saat esityksen käyttöön valitsemalla valikon ”Esitys” alta ”Mukautettu esitys”.

Avainsanat: tietoturva, tietojenkäsittely, terveydenhuolto, koulutus, henkilöstökoulutus

Sisällys

JOHDANTO

Taustaa

Tietoturvakoulutuksen materiaali on laadittu osana kansallista terveysprojektia ja tietoturvan alueellista toimeenpanoa projektityönä. Työ on tehty vuoden 2006 aikana. Materiaalin yksityiskohdat on esitetty jäljempänä. Työ on tehty yhteistyöryhmässä, jonka käytännön työtä on johtanut Stakesin Tero Tammisalo. Työn valvojana on toiminut Päivi Hämäläinen ja työryhmän sihteerinä Emmi Tenhunen, molemmat Stakesista. Koulutusmateriaalin laadintaan osallistuneet työryhmän asiantuntijajäsenet ovat Komula Ville (TYKS), Korhonen Maritta (KUH), Körkkö Pentti (PPSHP), Nevalainen Pekka (PKSSK).

Koulutusmateriaalin toimivuutta on testattu useissa erillisissä pilottikoulutustilaisuuksissa. Näissä on kysytty osallistujien kokemuksia ja pyydetty kommentteja materiaalin kehityksen avuksi ja tueksi. Koulutukseen on osallistunut arviolta 1 000 henkilöä, ja kommentteja on saatu lähes 200 osallistujalta. Materiaalia on muokattu ja kehitetty saatujen kommenttien perusteella.

Käyttötarkoitus

Koulutusmateriaali on laadittu osana tietoturvan alueellista toimeenpanoa: tarkoituksena on ollut tietoturvan yleisen tason parantaminen ja terveydenhuoltoon osallistuvien henkilöiden tietoturvatietoisuuden lisääminen. Edellä mainitut suureet ovat yhtäältä erittäin vaikeasti mitattavissa (monipuoliset ja toistetut testit kattavalle joukolle eri rooleissa toimivia ammattilaisia, kaiken kaikkiaan suurelle määrälle henkilöitä), mutta toisaalta tietoturvaosaamisen tason on todettu olevan uhka tietoturvalle ja tietosuojalle. Käytettävissä olevat resurssit, koulutuksen tarve ja aikataulupaineet huomioiden materiaali on laadittu ilman täsmällistä analyysiä siitä,

- keiden on tarkoitus osallistua järjestettäviin tietoturvakoulutuksiin, ja
- millaisia tietoja koulutukset sisältävät.

Pyrkimyksenä on siten ollut laatia yleispätevä materiaali, jota voidaan käyttää osana ensivaiheen jalkauttamistyötä tietoturvan kehittämisessä terveydenhuolloneri organisaatioissa. Materiaali on käytettävissä kouluttajien apuna kussakin organisaatiossa.

Materiaaliin ja koulutuksiin täytyy lisätä aineistoa organisaatiokohtaisesti: paketti ei sisällä riittävästi tietoa esimerkiksi potilastietojen käsittelyyn (kussakin organisaatiossa on omat potilastieto- ja kertomussovellukset, samoin kuin omat tietojen arkistointiprosessit) eikä päivittäiseen tietojärjestelmien käyttöön liittyen (kussakin organisaatiossa on esimerkiksi omat kulunvalvontasäännöt sekä tietokoneiden, tietoverkkojen, sähköpostien ja muiden sovellusten käyttöohjeistukset ja menettelytavat).

Materiaali ei sisällä lainsäädäntöön liittyviä yksityiskohtia: näiden lisääminen materiaaliin edellyttäisi kouluttajalta tietoturvaosaamisen lisäksi sellaista juridista osaamista, jota tietoturvakouluttajalla ei välttämättä ole. Kouluttaja voi toki oman osaamisensa perusteella tuoda esiin lainsäädännön yksityiskohtia, mikäli näkee tämän tarpeelliseksi. Myöskään koulutukseen osallistujilla ei ole välttämättä minkäänlaista juridiikan tuntemusta, joten liiat yksityiskohdat voivat mennä hukkaan ja sekoittaa osallistujia turhaan. On syytä tiedostaa, että käytännön työtä tehdään tyypillisesti tietojärjestelmillä, ja siten lain kirjain tulee yleensä toteutettua juuri niin kuin käytössä olevat tietojärjestelmät sen tekevät mahdolliseksi.

Edellisten lisäksi on myös tiedostettava, että henkilöstöllä voi olla huomattavaa tietoteknistä osaamisen ja tiedon puutetta. Siksi tietoturvakoulutuksessa on syytä välttää myös liiallista teknisten seikkojen korostamista.

On siis huomattava, että tämä koulutusmateriaali ei ole oppimateriaali. Sen perusteella ei voi sanoa, että koulutukseen osallistuja olisi saavuttanut tietyn tietoturvaosaamisen tason. Koska materiaalista puuttuu oleellinen osa organisaatiokohtaisesti tarvittavia tietoja, pelkästään tämän materiaalin perusteella annetun koulutuksen onnistumista ei sellaisenaan ole hyödyllistä mitata yksilötasolla.

Koska saatavilla on kuitenkin tutkimustietoa, että jo pelkästään tietoturvakoulutuksen määrä vähentää tietoturvauhkia ja parantaa siten tietoturvan tasoa, on suositeltavaa, että jokaisessa organisaatiossa otetaan käyttöön tietoturvan koulutusohjelma, jonka osana annetaan tietoturvakoulutusta organisaation koko henkilöstölle. Tämä materiaali tukee osaltaan tällaisen ohjelman käynnistämistä.

Materiaali

Materiaali sisältää seuraavat dokumentit:

- Koulutusmateriaali
  - Materiaalissa on mukana sekä PowerPoint- (Tietoturvakoulutus, esitysmateriaali.ppt) että pdf-muotoinen (Tietoturvakoulutus, esitysmateriaali.pdf) dokumentti. Lisäksi luennoijaa varten on luotu dokumentti Tietoturvakoulutus, esitysmateriaalin muistiinpanot.pdf.
  - PowerPoint-muotoinen esitys sisältää sekä luennoijan muistiinpanosivut että kaksi erillistä mukautettua esitystä: johto ja organisaatio. Diat johto-esitykseen on valittu lähinnä päätöksentekijöille annettavaa koulutusta ajatellen, organisaatio-diat taas sopivat koko henkilöstölle annettavaan koulutukseen. On toki suotavaa muodostaa diaista myös räätälöity esitys kohderyhmän tarpeiden tai luennoijan mukaan. Esityksessä on hyödynnetty PowerPoint-sovelluksen ominaisuuksia, esimerkiksi linkkejä muihin diaihin (mukaan lukien paluulinkit) sekä tekstien ja kuvien esiintuloa yksi tai osa kerrallaan (klikkauksesta).
  - Pdf-muotoinen esitysmateriaali ei sisällä luennoijan muistiinpanoja ja on sellaisenaan yksi kokonaisuus: mukautetuista esityksistä ei ole luotu omia dokumenttejaan. Muistiinpanot on luennoijan helpottamiseksi julkaistu myös omassa pdf-dokumentissaan (kts. yllä).
- Harjoitustehtävä
  - Koulutuksen yhteydessä tehtävää harjoitusta varten on laadittu kysymyslomake (Tietoturvakoulutus, kysymyslomake.pdf) ja vastauslomake (Tietoturvakoulutus, vastauslomake.pdf). Molemmat on saatavissa myös Word-muodossa.
  - Luennoijaa varten on laadittu oikeat vastaukset ja pohdintaa sisältävä dokumentti (Tietoturvakoulutus, oikeat vastaukset.pdf) joka on saatavissa myös Word-muodossa.
  - Harjoitus on osa koulutusta, eikä sitä voi käyttää osallistujien testaamiseen. Vuorovaikutteisen harjoituksen on havaittu lisäävän oppimista ja ylläpitävän motivaatiota. Pilottikoulutuksissa tehdyissä kyselyissä harjoitustehtävä koulutuksen yhteydessä koettiin erityisen mielekkääksi.

Koulutus

Pilottikoulutuksissa havaittiin, että parhaan lopputuloksen saamiseksi koulutustilaisuus kannattaa järjestää ”puolen päivän seminaarina”, jolloin arviolta 3–3,5 tunnin jakso sisältää seuraavat aihealueet:

- Tietoturvallisuuden perusteet ja lainsäädäntö (50 minuuttia ja 10 minuutin tauko).
- Organisaatiokohtaiset säännöt, sovellukset ja tietotekniikka (50 minuuttia ja 10 minuutin tauko).
- Harjoitustehtävä ja vastausten läpikäynti (tehtävä 30 minuuttia, vastausten läpikäynti ja keskustelu osallistujista riippuen 30 minuutista tuntiin asti).

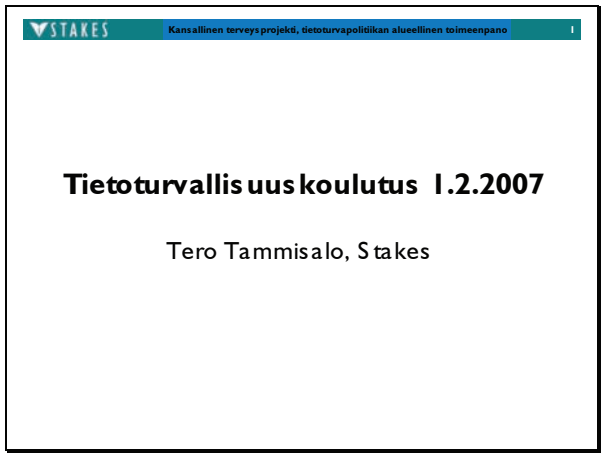
Tällaisten seminaarityyppisten koulutusten lisäksi on suositeltavaa toteuttaa erilaisia pienempiä koulutustilaisuuksia ja tietoiskuja aina tarvittaessa. On myös suositeltavaa, että tietoturvan koulutusohjelmaan osallistuminen säädetään pakolliseksi koko organisaatiolle.

Seuranta

Jos organisaatiossa nähdään tarpeelliseksi, voidaan yleistä tietoturvaosaamisen tasoa ja mahdollista muutosta mitata tilastollisesti harjoitustehtävän avulla, jos vastauslomakkeet kerätään ja tulokset kirjataan. Vastauslomakkeet on kerättävä nimettöminä: harjoitustehtävää sellaisenaan ei ole suunniteltu käytettäväksi yksittäisen osallistujan osaamisen mittarina.

Koulutusdiat muistiinpanoineen

DIA 1



Esityksen ajankohdan ja luennoitsijan nimen saa muuttaa oman koulutustilaisuuden mukaiseksi. Luennoitsijan esittäytyessä hänen toivotaan myös esittelevän lyhyesti projektin, jonka tuotoksena koulutussuunnitelma ja koulutus on toteutettu. Kyseessä on kansallisen terveysprojektin hanke, jossa ovat mukana Tero Tammisalo ja Emmi Tenhunen/Stakes, Ville Komula/TYKS, Maritta Korhonen/KYS, Pentti Körkkö/PPSHP, Pekka Nevalainen/PKKSH. Hanke on tehty STM:n ohjauksessa ja on jatkoa aiemmin tehdylle tietoturvaohjeistukselle.

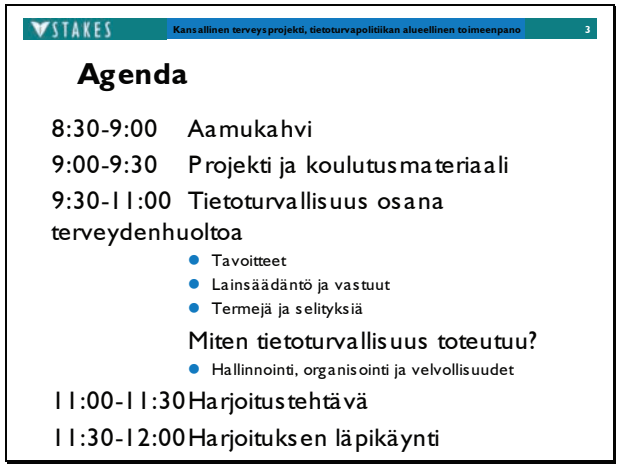
Koulutusmateriaalin laadinnassa on otettu soveltaen huomioon Valtiovarainministeriön julkaisu Opas julkishallinnon tietoturvakoulutuksen järjestämisestä (VAHTI 6/2003).

Tämän koulutuksen tavoite on saada koulutukseen osallistuja ymmärtämään tietoturvallisuuden tärkeys ja saada hänelle ”tietoturvallisen ajattelutavan siemen itämään”. Tavoite on myös kertoa ne oleellisimmat asiat, joiden avulla osallistuja voi omassa työssään edesauttaa tietoturvallisuutta, ja kertoa hänelle tärkeimmät säännöt, jotka hänen täytyy työssään huomioida.

Tavoite ei ole tarkkojen toimintaohjeiden eikä täsmällisen teknologisen tai juridisen tiedon välittäminen. Vasta, kun osallistujalle onnistutaan istuttamaan edellä mainittu ”tietoturvallisen ajattelun siemen”, hän on valmis omaksumaan mallin oikeanlaiseen käyttäytymiseen ja toimintaan. Silti, vaikka tässä vaiheessa täsmällisten vaatimusten esittäminen olisi jopa turhaa, on esityksen muistiinpanosivuilla esitetty teknisiä yksityiskohtia, jos joku kuulijoista sellaisia kysyy tai jos luennoija haluaa esittää esimerkkejä.

Esityksessä on kaksi valmista mukautettua esitystä: johto ja kouluttajat. Niihin on valittu osajoukko dioista.

DIA 2



Diassa 2 on esimerkki puolen päivän pituisen tietoturvakoulutuksen ohjelmaksi.

Kuulijat voivat esittää kysymyksiä joko koulutuksen aikana tai sen lopussa, jolloin pidetään vielä erillinen keskusteluosuus tietoturvakysymyksistä.

Eri aiheiden lomassa esitetään muutamia käytännön esimerkkejä tietoturvaloukkauksista.

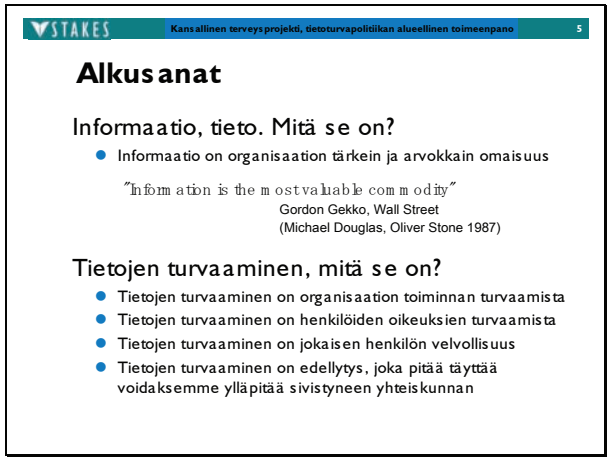
ORGANISAATION KOULUTUS: Harjoitustehtävän aikana kysymykset eivät ole sallittuja, elleivät ne ole lomakkeen täyttöön liittyviä.

JOHDON KOULUTUS: Keskusteluosuus sisältää myös muutaman aiheeseen liittyvän kysymyksen, jotka voidaan käydä läpi ryhmätyönomaisesti.

DIA 3

Seuraavilla dioilla käydään läpi mitä tietoturvallisuus on, ja esitetään aiheesta muutama esimerkki.

DIA 4

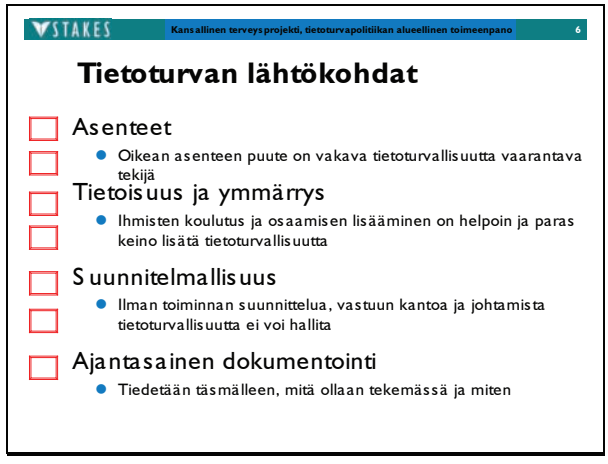


Käytännössä jokaisen organisaation tai yrityksen toiminta perustuu tavalla tai toisella erilaisten ja eri muodossa olevien tietojen olemassaoloon ja hyväksikäyttöön.

Tietojen käsittely, siihen liittyvät vaatimukset ja myös viranomaisen toiminta (hyvä tiedonhallintatapa) on kirjattu myös useaan lakiin, joista edempänä esityksessä.

Tieto on perinteisen (epistemologia, filosofian tietoteoria) näkemyksen mukaan tosi, hyvin perusteltu uskomus. Pelkkä tosiasia ei sellaisenaan ole tieto; ei ainakaan sellainen tieto jota pitäisi suojata. Myöhemmin käsitellään lisää sitä, millaisia tietoja ylipäätään tulee suojata. Erilaisia mittauksiahan voidaan tehdä loputtomasti ja saatavia mittaustuloksia olisi ääretön määrä, joten tiedon määrä on ääretön. Suojattavan tiedon määrä on kuitenkin erittäin rajallinen.

DIA 5



Heti aluksi on hyvä tähdentää, että tietoturvallisuudesta huolehtiminen on lakisääteistä toimintaa.

Tietoturvallisuus syntyy ennen kaikkea oikeanlaisista asenteista ja oikeasta asennoitumisesta. Välinpitämättömyys on vakava uhka, oli se tietoinen tai tiedostamaton asenne.

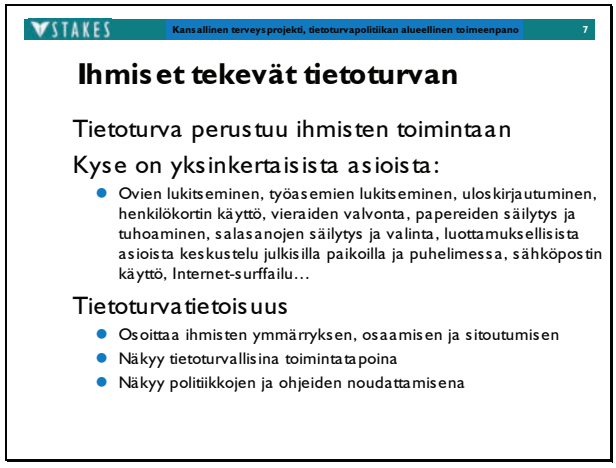
ASENTEET, TIETOISUUS JA YMMÄRRYS: koulutus ja määräajoin tapahtuva kertaus koko organisaatiolle; tietoturvallisuuden mielessä pitäminen (huoneentaulut, muistutusviestit, ym.) ja riittävä osaamistaso (koulutus, tietoturvamanuaali).

SUUNNITELMALLISUUS on organisaation johdon vastuulla.

AJANTASAINEN DOKUMENTOINTI: sen ylläpito on osa päivittäistä tietojärjestelmien ja tietoturvallisuuden hoitoa.

Punaisissa neliöissä on linkki kunkin aliotsikon mukaiseen esimerkkiin. Esimerkistä pääset kyseisellä dialla olevalla linkillä takaisin.

DIA 6



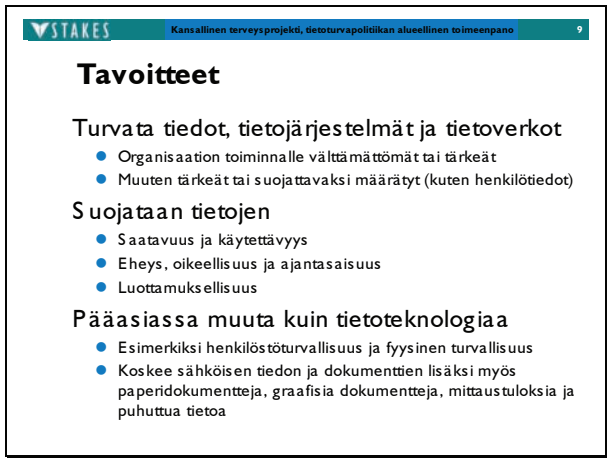
Tietoturvallisuuden perusta, oleellisin tekijä, on ihminen.

Ihmisen toiminta on tyypillisin uhka tietoturvallisuudelle, niinpä ihmisen oikeanlaisen toiminnan takaaminen on myös paras suojauskeino.

DIA 7

Seuraavilla dioilla käydään läpi tietoturvallisuuden tavoitteita ja asioita, joista tietoturvallisuus koostuu.

DIA 8

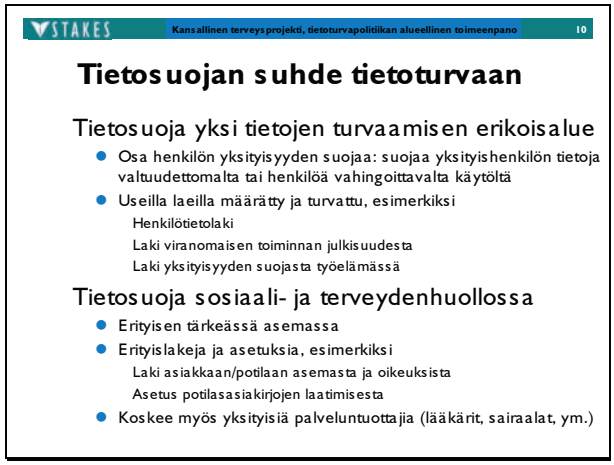


Turvataan tärkeiden tietojen olemassaolo. Tämä edellyttää, että on tiedossa, mitkä ja millaiset tiedot ovat välttämättömiä ja tärkeitä. Jotta tiedot voidaan turvata, pitää tietää uhkat ja riskit, joita tietoihin kohdistuu. Sen jälkeen voidaan valita oikeat ja oikein mitoitetut suojaamistoimenpiteet. Tämä on tietoturvasta huolehtivan organisaation tehtävä, jota selvennetään tarkemmin jäljempänä. Koska tietoturvallisuus ei koske ainoastaan sähkömuotoista tietoa ja IT- tai ATK-järjestelmiä, tietoturvallisuuden organisoinnin ei pitäisi olla tietohallinnon alainen vaan suoraan organisaation ylimmän johdon alaisuudessa. Pääasia tietoturvallisuudessa ei ole teknologiaa vaan ihmisten johtamista. Yleensä parhaatkin menettelyt ja teknologiat voidaan kiertää, kun on riittävä osaaminen.

Saatavuus (availability) eri asia kuin käytettävyys (usability). Käytettävyys voi estyä, vaikka tiedot olisivat saatavilla, jos esimerkiksi uudet ohjelmistot eivät voi käyttää vanhoja tiedostomuotoja, vanhoja tietovälineitä ei voida käyttää ym. Eheä tieto (integrity): tieto ei ole muuttunut (ohjelmistovirheet, tahalliset tai tahattomat käyttäjän virheet), se on ajantasaista ja oikeaa, alkuperäisyys voidaan todeta. Kiistämättömyys (non-repudiation) toteutetaan esimerkiksi sähköisellä allekirjoituksella (digital signature) ja aikaleimalla (time stamp). Luottamuksellisuus (confidentiality): sivulliset eivät saa päästä tietoihin käsiksi. Tähän liittyy myös oikeanlainen tietojen käyttötarkoitus. Terveydenhuollon ammattihenkilö ei saa käyttää tietoja ilman asianmukaista tarkoitusta: ei riitä, että hänellä on niihin pääsy (pääsyoikeus; access right, user right). Esimerkiksi hoitajalla, jolla on pääsy potilastietojärjestelmään, ei ole oikeutta tarkastella tietoja, ellei hoitosuhde luo sille perusteita.

Tietojen käytön säännöt (käsittely, säilytys, poisto, siirto, luovutus ym.) toteutetaan esimerkiksi pääsynhallinnalla (access control): käyttäjät tunnistetaan ja todennetaan (identification, authentication) ja heille myönnetään identiteettiin, asemaan ja työtehtävään perustuva rooli ja sen mukaiset käyttövaltuudet tietoihin.

DIA 9



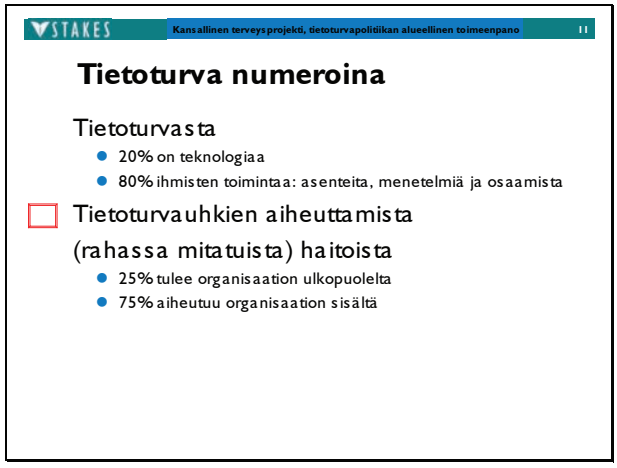
Tietosuoja ja tietoturva eivät ole toisensa poissulkevia vaan täydentävät toisiaan. Tietoturvallisuuden toteuttaminen ja siinä käytettävät menetelmät ja teknologiat on laaja kokonaisuus, joka sisältää kaiken organisaatiolle tärkeän tiedon turvaamisen toimenpiteet (mukana esim. rahoituksen ja kirjanpidon tiedot ja erilaiset toimintaan liittyvät suunnitelmat ja muut dokumentit).

Tietosuoja puolestaan on juridinen termi, jolloin tarkoitetaan nimenomaan henkilötietoihin (esim. potilastiedot) kohdistuvaa suojaa ja tällaisten tietojen käyttöä.

Voikin sanoa, että tietoturvallisuudella toteutetaan (muun muassa) tietosuojan vaatimuksia. Toki myös muita tietoturvaan liittyviä vaatimuksia löytyy, eikä näitä ole ainakaan tässä yhteydessä syytä priorisoida. Sekä tietoturvaa että tietosuojaa säädellään laeilla ja määräyksillä.

Suomen lainsäädännöstä ja laeista on saatavilla tietoa myös Internetissä, osoitteessa www.finlex.fi.

DIA 10



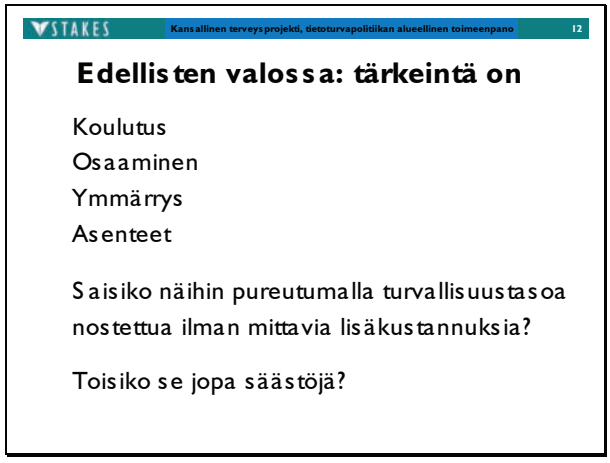
Luvut ovat usein esillä tietoturvaan ja riskienhallintaan liittyvissä esityksissä. Ne ovat säilyneet lähivuosina kohtuullisen muuttumattomana, mutta lisääntyneiden verkko-ongelmien ja lainsäädännön uusiutumisen myötä 25–75 suhde on viime aikoina voinut muuttua ulkopuolelta aiheutuvien kustannusten suuntaan. Tällaisia lukuja ei kuitenkaan ole vielä saatavilla.

25–75-luku on haittojen rahallisen arvon suhde (turvaluokittelussa tiedon rahallinen arvo ei välttämättä ole määräävä; myös tiedon merkitys voi olla ratkaiseva, kuten esimerkiksi poti-

lastietojen ollessa kyseessä). Luku on saatu Infoworldin verkkosivuilta. Suora lainaus: ”Studies from the Computer Security Institute/FBI, U.S. Congress, Gartner, and others estimate that as much as 75 percent of the $200 billion in measured annual security losses comes from within organizations.”

Punainen neliö on linkki diaan ”hyvä tiedostaa”, joka on hyvä näyttää tässä kohdassa. Se sivuaa tietoturvainvestointeja ja erityisesti sitä, mihin rahat laitetaan: teknologiaan vai ihmisten johtamiseen.

DIA 11



Pari retorista kysymystä.

DIA 12

Seuraavilla dioilla esitellään lyhyesti asiaan liittyvää lainsäädäntöä.

Tässä kohdassa voi yleisölle esittää minuutin miettimistehtävän ja käydä lyhyen keskustelun asiasta:

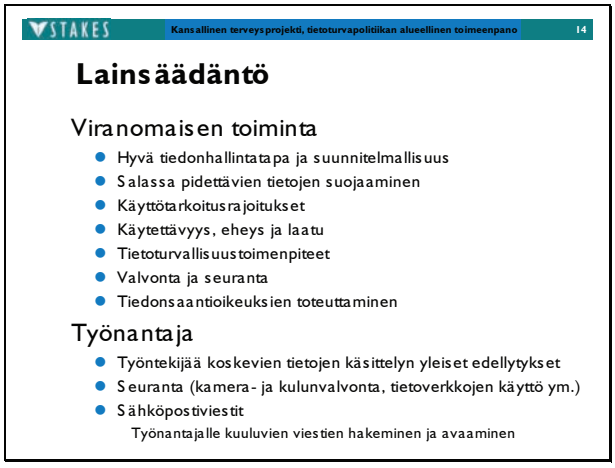
”MITÄ TIETOJA ILMAN ET VOISI SUORIUTUA TYÖSTÄSI?”

”MIKSI? MIHIN TARVITSET KYSEISIÄ TIETOJA?”

”MITEN EM. TIETOJA SUOJATAAN, JA … MITEN NIITÄ TULISI SUOJATA?”

Osallistujia voidaan pyytää listaamaan tietoja paperille. Listasta pitäisi syntyä käytännön järjestelyihin liittyviä tietoja (”missä työhuone sijaitsee”, ”missä leikkaussali sijaitsee” ym.), ammatilliseen osaamiseen/koulutukseen liittyviä tietoja, ja työprosesseihin sekä työn tekemiseen liittyviä tietoja (potilaan tiedot, järjestelmien käyttöohjeet ym.).

DIA 13



Näillä dioilla ei käsitellä yksityiskohtia laeista, eikä listata kaikkia tietoturvaan ja tietosuojaan liittyviä lakeja. Sen sijaan esityksen aikana tulee esiin oleellisia, lakeihin perustuvia seikkoja, jotka jokaisen on tiedostettava ja tiedettävä toimiessaan ammatissaan.

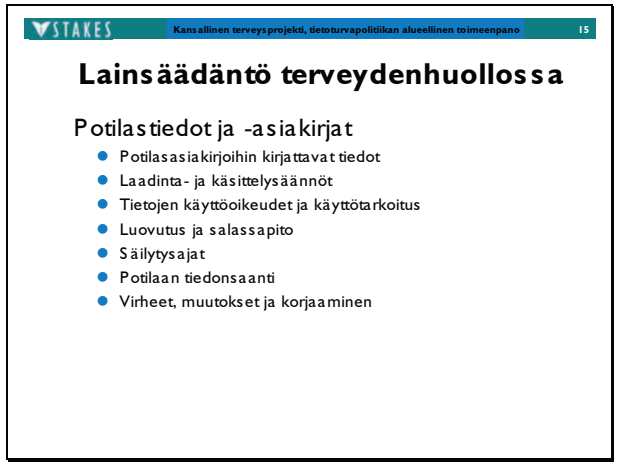
Seuraavassa vain yleiskatsaus, millaisista asioista tietoturvallisuuteen liittyen ylipäätään on voimassa olevaa lainsäädäntöä.

Lait edellyttävät viranomaistoimijan noudattavan hyvää tiedonhallintatapaa. Hyvästä tiedonhallintatavasta on laissa selkeät määrittelyt ja tietoturvan ylläpito on erikseen mainittu tässä yhteydessä.

Työnantajaa koskevat tietyt velvoitteet työntekijän tietojen käsittelyyn liittyen. Näistä on säädetty erillisillä laeilla (huomaa myös yhteistoimintalaki, laki turvallisuusselvityksistä). Samoin on säädetty myös asiakkaiden/potilaiden tietoihin liittyvistä asioista. Nämä lait voivat kuulua esimerkiksi sosiaali- ja terveydenhuollon erityislakien, henkilötietolain tai sähköisen viestinnän tietosuojalain piiriin.

Lait turvaavat myös työntekijän – terveydenhuollon ammattihenkilön – oikeusturvaa.

DIA 14

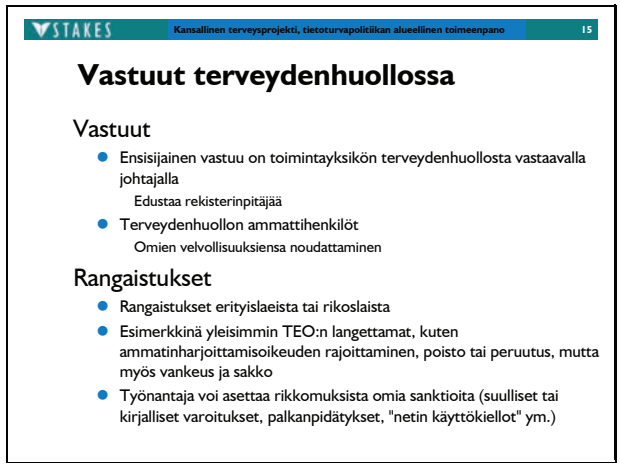


Potilasasiakirjoja (ja sosiaaliturvan asiakkaaseen liittyviä asiakirjoja) ja niissä olevia tietoja on suojattava erikseen. Niiden käsittelyä koskevat monet lisävaatimukset, joita ei muiden henkilötietojen käsittelyyn liittyen ole.

Erityisesti potilasasiakirjojen laatimista sekä niiden ja muun hoitoon liittyvän materiaalin säilytyksestä on säädetty muihin toimialoihin verrattuna poikkeuksellisia säilytysaikoja erillisellä asetuksella. Vastuu on määritelty rekisterinpitäjälle, josta lisää seuraavassa diassa.

Muutoin esimerkiksi asiakkaan tiedonsaantioikeus omista tiedoistaan sekä oikeus virheiden korjaamiseen ovat vastaavat kuin henkilötietolaissa.

DIA 15



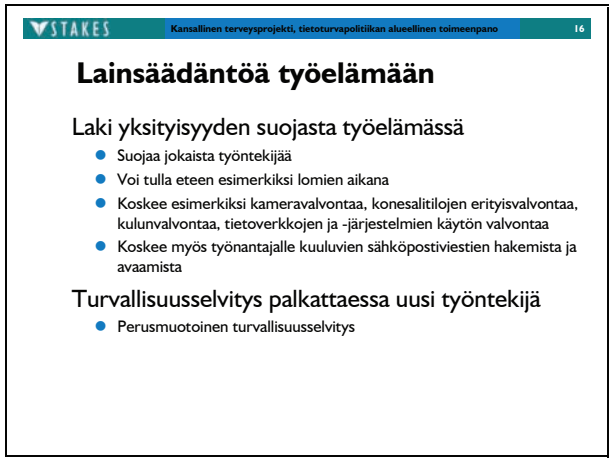
Toimintayksikön terveydenhuollosta vastaava johtaja toimii rekisterinpitäjän edustajana ja on siten vastuullinen henkilö. Hänen vastuulleen kuuluu, että toimintayksikössä on käytössä ja koulutettuna tietojen ja asiakirjojen laatimiseen, käsittelyyn ja säilytykseen liittyvä ohjeistus ja tarvittavat määräykset.

Työnantaja vastaa luonnollisesti esimerkiksi sähköpostiviestien tai verkkoliikenteen tarkastamisen ja seurannan lainmukaisuudesta.

Kutakin työntekijää sitovat lakien lisäksi hänen työnantajansa kanssa solmimat sopimukset (työsopimus, salassapitosopimus, ym.) ja niissä huomioidut organisaatiossa voimassa olevat määräykset ja ohjeet.

”Esimies ja tietoturva”: Tässä voi näyttää esimerkkiä. Turvallisuusasioihin liittyviä rangaistuksia ei tule käyttää vallankäytön välineenä (esimerkiksi ”nettikielto” muusta syystä kuin netin väärinkäytöstä ym.). Yhdenmukaisuuden periaatetta tulee noudattaa (jos yhdellä henkilöllä on pääsy nettiin ilman, että hän tarvitsee nettiä työssään, saman pitäisi olla sallittu kaikille).

DIA 16



Lakeja esimerkiksi Laki yksityisyyden suojasta työelämässä (13.4.2004/759) ja Laki turvallisuusselvityksistä (8.3.2002/177).

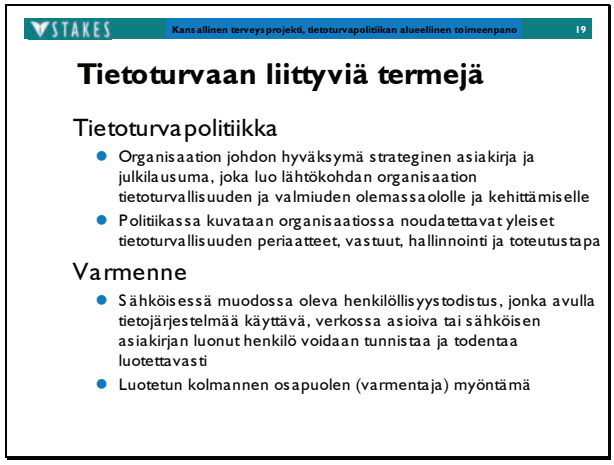
Mainitut asiat saattavat usein tulla eteen esimerkiksi esimiesasemassa oleville.

Perusmuotoinen turvallisuusselvitys: poliisiasiain tietojärjestelmä, rikosrekisteri, liiketoimintakieltorekisteri, oikeushallinnon tietojärjestelmät, pääesikunnan pitämiin rikostietorekisteriin ja turvallisuustietorekisteriin, rajavartiolaitoksen esikunnan pitämään virka-apurekisteriin, tullihallituksen pitämään virka-apujärjestelmään, väestötietojärjestelmään ja ulkomaalaisrekisteriin.

DIA 17

Seuraavilla dioilla on esitetty muutamia tietoturvaan, tietosuojaan ja potilastietoihin liittyviä termejä.

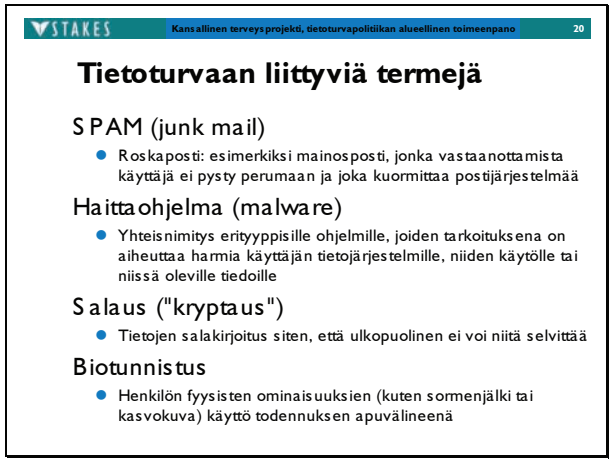
DIA 18



Kuulijoita ohjeistetaan siten, että jos mielessä oleva termi, joka aiheuttaa epäselvyyksiä, ei esiinny tällä tai parilla seuraavista dioista, sitä kannattaa ehdottomasti kysyä.

Varmenteeseen liittyy lisäksi paljon muutakin yleisesti käytettyä termistöä, osa seuraavista on jo aiemmin mainittu: PKI (public key infrastructure, julkisen avaimen infrastruktuuri), sertifikaatti, CA (certificate authority), TTP (trusted third party), sähköinen allekirjoitus, aikaleima, kiistämättömyys, vahva tunnistus ja todennus, sulkulista, mitätöinti (revocation), julkinen avain (public key), salainen avain (private key), toimikortti, älykortti, ym.

DIA 19



Haittaohjelma voi poistaa tai muuttaa ohjelmia ja tietoja käyttökelvottomiksi, avata uusia tietoliikenneyhteyksiä ilman käyttäjän lupaa tai vakoilla (spyware) käyttäjän toimia esimerkiksi tallentamalla näppäinten painallukset. Erittäin usein haittaohjelmat liittyvät sähköpostin ja erityisesti liitetiedostojen käyttöön (virukset) tai verkkotunkeutumisiin. Näitä vastaan suojaudutaan esimerkiksi virustorjunnalla, palomuureilla ja tunkeutumisen tunnistimilla (IDS, intrusion detection) ja varsinkin KÄYTTÄJÄN OIKEANLAISELLA TOIMINNALLA.

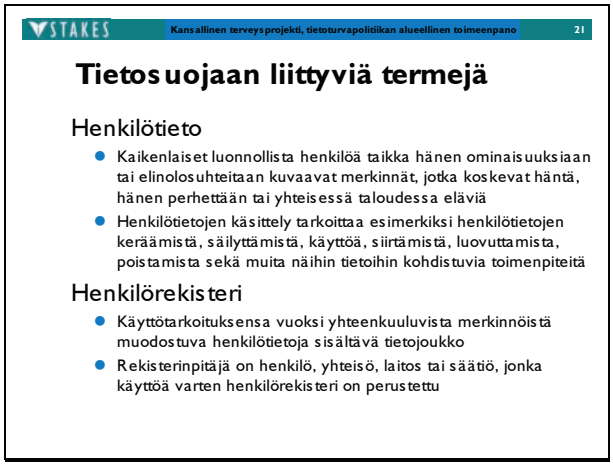
Salaus (encryption) ja sen purku ovat yksi edellä mainitun julkisen avaimen infrastruktuurin sovelluksia.

Esimerkiksi normaalissa henkilökortissa tai passissa olevaa biotunnistetta (valokuva) on käytetty henkilön identiteetin todennukseen jo vuosikymmeniä. Sähköiseen maailmaan siirret-

tynä vastaava menettely on huomattavasti helpompaa ja käytännöllisempää toteuttaa käyttämällä esimerkiksi sormenjälkitunnistetta: sormenjäljen vertaaminen sen sähköiseen muotoon on huomattavasti kätevämpää kuin kasvokuvan.

Internetissä on uusia hyökkäystyökaluja ja -menetelmiä, mm. virusten levittäminen roskapostin avulla sekä phishing (käyttäjä- ja salasanatietojen kalastus aidon näköisillä sivustoilla), jotka usein hyödyntävät selainten haavoittuvuuksia ja turvaominaisuuksien puutteita sekä käyttäjien tietämyksen puutteita. Internet-uhkat ovat usein ammattimaisia (myös järjestäytynyttä rikollisuutta) ja tavoitteena on myös tietojenkäsittelykapasiteetin ja -resurssien hyväksikäyttö, ei pelkästään pääsy tietoihin.

DIA 20



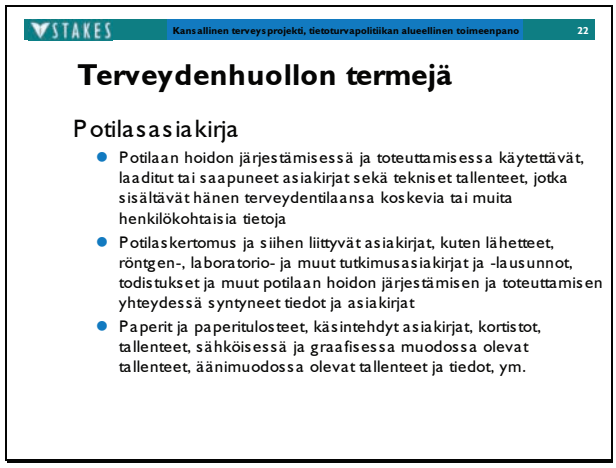
Määritelmät Henkilötietolain (22.4.1999/523) 3 §:stä. Muita määritelmiä 3 §:stä alla.

Huomaa, että henkilörekisteri on käyttötarkoitussidonnainen. Huomaa myös rekisteröidyn tarkastusoikeus ja informointivelvoite.

Rekisteröity on se henkilö, joita henkilörekisterissä olevat henkilötiedot koskevat. Sivullinen on kuka tahansa muu kuin rekisteröity, rekisterinpitäjä tai henkilötietojen käsittelijä.

Suostumus on vapaaehtoinen, yksilöity ja tietoinen tahdon ilmaus, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.

DIA 21



Terveydenhuollon tietosuojaan yksi oleellisimmin liittyvistä termeistä on potilasasiakirja. Siitä on tässä kolme diaa.

Määritelmät: Laki potilaan asemasta ja oikeuksista 17.8.1992/785 (2 §) sekä STM:n asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä. Asetus tullaan uudistamaan vuoden 2007 aikana.

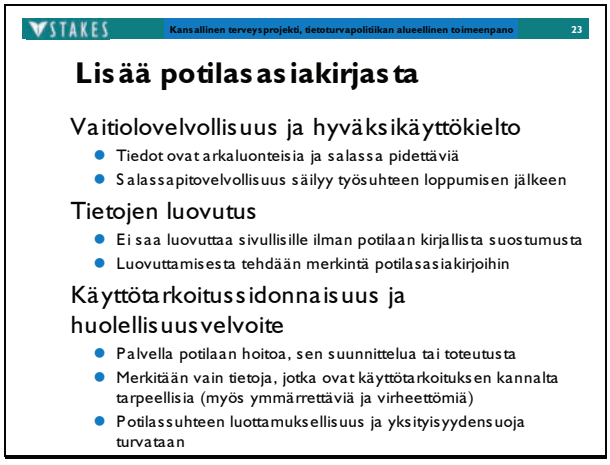
Asetus koskee terveydenhuollon ammattihenkilöitä (kuten terveydenhuollon ammattihenkilöistä säädetyssä laissa 559/1994 tarkoitetaan) heidän antaessaan terveyden- ja sairaanhoitoa riippumatta siitä, kenen palveluksessa ammattihenkilö on tai harjoittaako hän ammattiaan itsenäisesti.

Huomaa, että ajanvaraustiedot yksilöivät henkilön ja niitä käytetään hoidon järjestämisessä: ne ovat potilastietoja.

Tässä kohdassa voi kysyä käytännön esimerkkin ”kahvihuonekeskustelusta”: kuinka moni kuulijoista on kuullut (tai puhunut) potilaan asioista kahvihuoneessa tai muussa tilassa, jossa ei voi olla varma, onko jokainen läsnäolija mukana hoitoprosessissa ja siten oikeutettu kuulemaan tietoja? Millaisilla paikoilla on tapana keskustella asioista, jotka sisältävät potilastietoja?

Siis myös puhuttua tietoa on suojattava ulkopuolisilta: läsnä olevat ulkopuoliset henkilöt (terveydenhuollon ammattilaiset, muut potilaat, omaiset ym.) voivat unohtua helposti, vaikka keskusteluissa käsiteltäisiin arkaluonteisia tietoja.

DIA 22

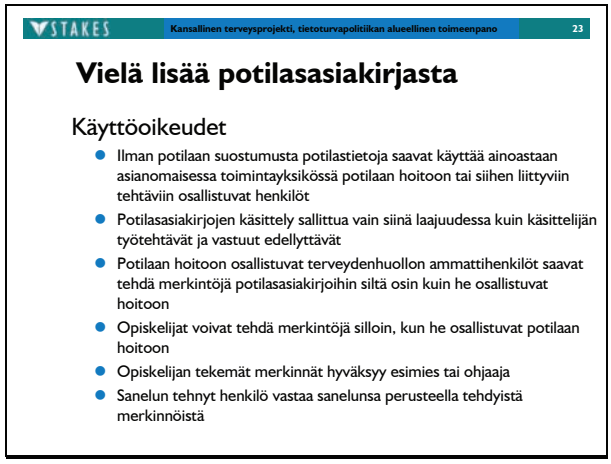


Edellisillä dioilla olevien lakien lisäksi on mainittava myös laki viranomaisen toiminnan julkisuudesta (21.5.1999/621).

Termi sivullinen käytiin läpi jo edellisillä dioilla. Tässä yhteydessä asiasta voi muistuttaa tai kysyä.

Merkittyjen tietojen tulee olla tarpeellisia, eivätkä ne saa olla virheellisiä, epätäydellisiä tai vanhentuneita. Tarpeettomat, puutteelliset, väärät, virheelliset ja vanhentuneet tiedot tulee korjata tai poistaa. Luonnollisesti korjaamisesta ja poistosta tulee tehdä tarvittavat merkinnät.

DIA 23



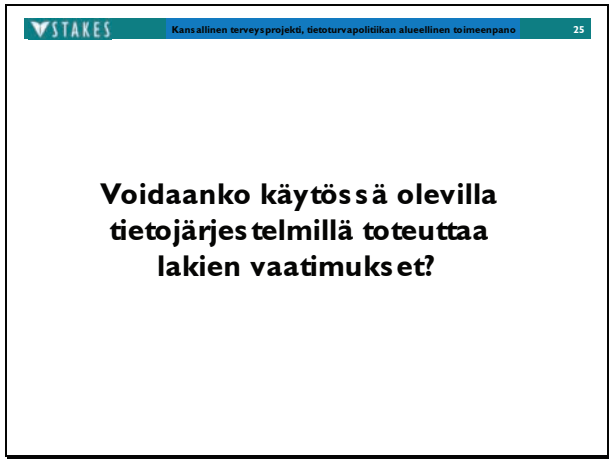
Määritelmät STM:n asetuksesta potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä.

Huomaa, että mahdollisuus ei tarkoita oikeutta. Tästä syystä esimerkiksi perheenjäsenten tietojen katsominen on kiellettyä, ellei hoitosuhdetta ole, vaikka katsomiseen tietojärjestelmän puolesta olisikin mahdollisuus.

Käyttöoikeudet on määriteltävä yksityiskohtaisesti. Käytössä olevilla resursseilla ei liene mahdollista rakentaa tekoälyä, joka määrittäisi reaaliaikaisesti ja automaattisesti kulloisetkin käyttöoikeudet siten, että ylimääräisiä mahdollisuuksia ei olisi. Siksi myös ohjeistus ja ohjeistuksen noudattaminen on välttämätöntä, ja käyttöä ja ohjeiden noudattamista valvotaan.

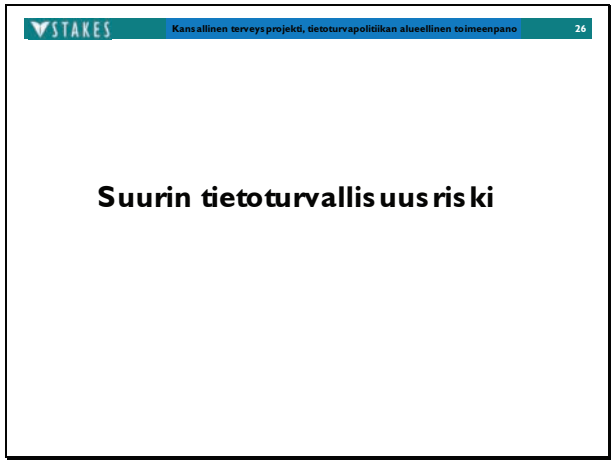
Terveydenhuollon ammattihenkilöiden lisäksi muut heidän ohjeidensa mukaisesti hoitoon osallistuvat henkilöt voivat tehdä merkintöjä potilasasiakirjoihin.

DIA 24



Yksi kysymys lisää mietittäväksi.

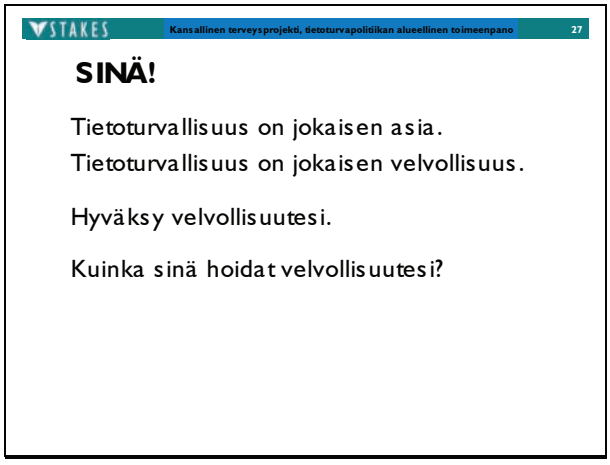
DIA 25



Yleisön ajattelun herättämiseksi voidaan kysyä, mikä on suurin tietoturvallisuusriski (tai uhka)?

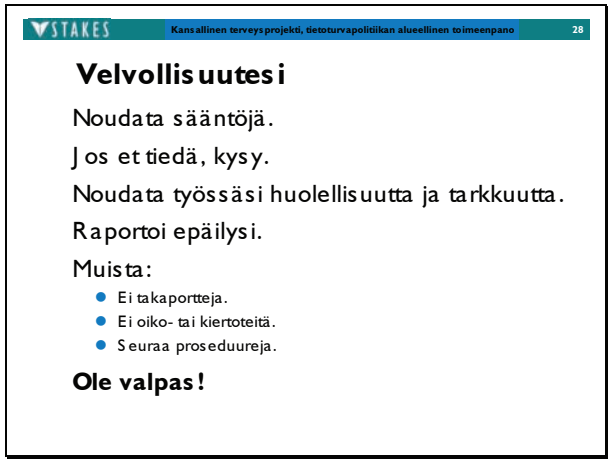
Johdon koulutuksessa kerrotaan, että tätä ja kahta seuraavaa diaa käytetään organisaation koulutuksen yhteydessä, provosointina ja ohjeena.

DIA 26



Jokaisen on ymmärrettävä omat velvollisuutensa, ja hyväksyttävä ne. Seuraavalla dialla on muutamia esimerkkejä kaikkien velvollisuuksista.

DIA 27



Kysyminen ei ole tyhmyyden merkki, päinvastoin. Jos ei tiedä, jos ei osaa tai jos on pieninkin epäilys, on parempi kysyä kuin tehdä ja katua myöhemmin.

Mainitse vielä kerran vakavat uhkat: huolimattomuus, kiire, piittaamattomuus, tietämättömyys.

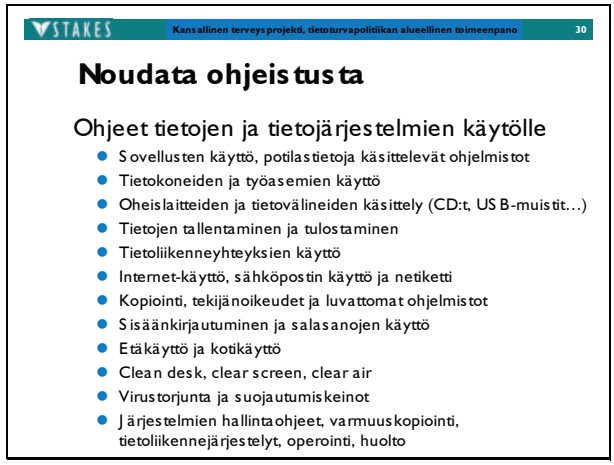
DIA 28

Seuraavilla dioilla on esimerkkejä erilaisista tietoturvallisuuteen liittyvistä ohjeista.

Tässä kohtaa voi kertoa alla olevan esimerkin tapahtuneesta.

Esimerkki (terveydenhuoltoalan) oppilaitoksesta: opiskelija lähettää opettajalle sähköpostia, jossa hän kertoo joutuvansa pitkälle sairaslomalle. Asiasta käydään hyvin henkilökohtaista keskustelua useassa viestissä, ja koko käyty keskustelu näkyy myös viimeisen viestin sisältönä. Opettaja päättää tiedottaa muita opettajia sairaslomasta edelleen lähettämällä viimeisen viestin saatteella varustettuna koko opettajakunnalle. Niinpä koko käyty keskustelu tulee tiedotettua jokaiselle opettajalle. Menikö kaikki niin kuin piti?

DIA 29

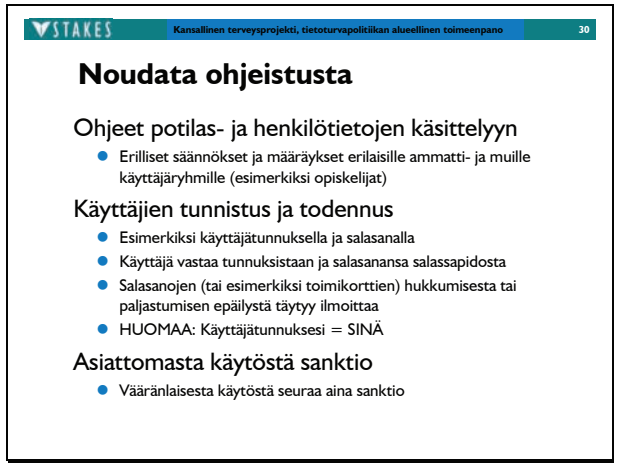


Kustakin mainitusta osakokonaisuudesta on erillinen ohjeistus tai se kuuluu osaksi yleistä tietoturvaohjeistusta. Teknisiä torjuntakeinoja ovat mm. palomuurit, virustorjunnat, liikenteen suodatus ja yhtenä tärkeimmistä varmuuskopiointi. Tässä yhteydessä kannattaa kysyä, onko mainituista ohjeista joku sellainen, jota ehdottomasti tarvittaisiin mutta jota ei ole käytettävissä.

Kannattaa mainita erilaisia esimerkkejä kustakin kokonaisuudesta. Tässä yhteydessä on esitettävä ohjeistusta erityisesti sovelluksiin, joissa käsitellään ja talletetaan potilas- ja henkilötietoja. Esimerkiksi:

- Sähköposti, liitetiedostot, virustorjunta ja luotettava alkuperä.
- Internetin käyttö: luotettavat, sallitut ja kielletyt sivustot, tiedostojen lataaminen, tekijänoikeudet ja virustorjunta.
- Yksityissähköpostin käyttö, käyttäjätunnukset ja salasanat.
- Salasanan valinta, salasanaa ei paperille, salasanan luovuttaminen ym. sääntöjä.
- Näytönsäästäjän ja lukituksen käyttö.
- Tietovälineiden (USB-muistit, CD- ja DVD-levyt, paperitulosteet, korput) käyttö, niille tallentaminen ja niiden hävittäminen.
- Työaseman käyttö ja ohjelmien tai lisälaitteiden asentaminen.

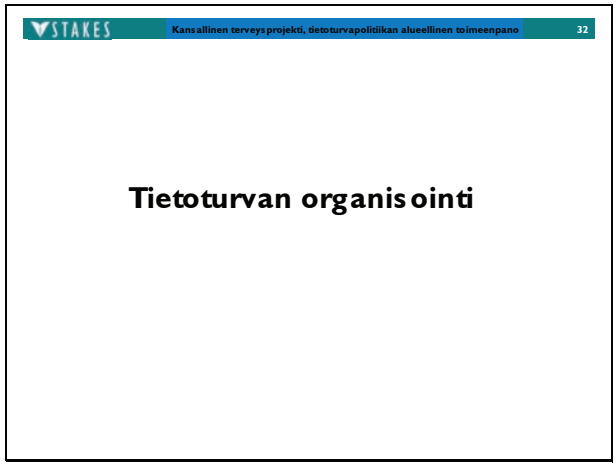
DIA 30



Käyttäjillä pitää olla

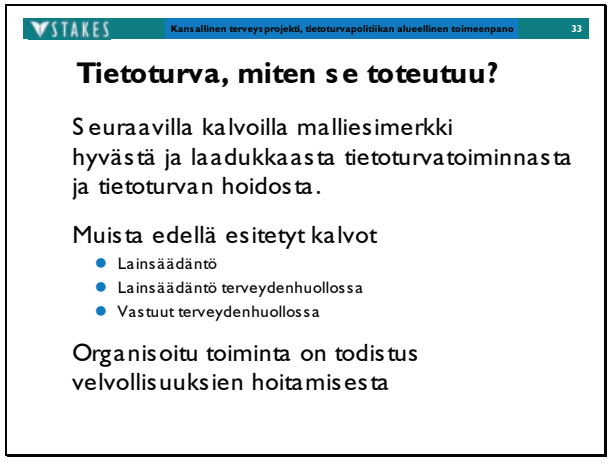
- riittävät tiedot (suojattavan tiedon tunnistaminen),
- riittävät taidot (salausohjelmien käyttö, virustorjunnan käyttö, tietojärjestelmien, sähköpostin ja Internetin oikeanlainen/sallittu käyttö)
- mahdollisuudet noudattaa ohjeita (kiire, työkuorma, työvälineet, teknologian toimivuus).

DIA 31



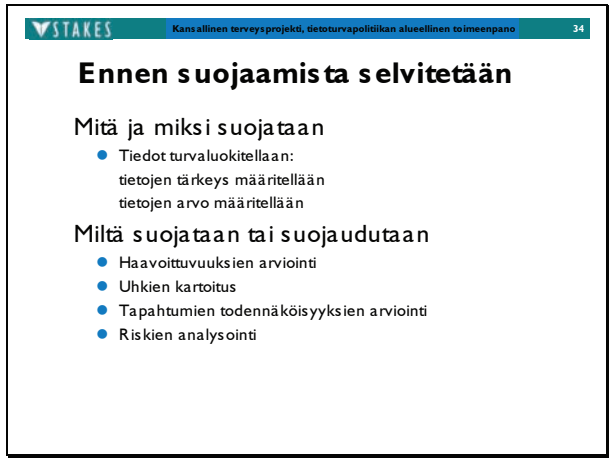
Seuraavilla dioilla on kuvattu esimerkinomaisesti tietoturvallisuuden organisointi ja hallinnointi organisaatiossa.

DIA 32



Hyviä esimerkkejä huonosta tietoturvallisuuden hoidosta on olemassa läjäpäin, kuten esimerkeissä on esitetty.

DIA 33

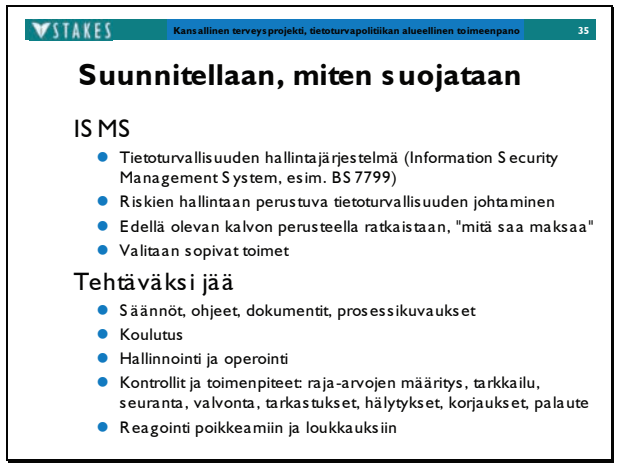


Tietoturvallisuutta toteutetaan ja sitä parannetaan suojaamalla, siksi diassa käytetään termiä ”suojata”.

Oleellinen asia suojauksen kannalta on tietää, mitä tietoja (ja miksi) ollaan suojaamassa. Toiseksi täytyy tietää, miltä suojaudutaan. Vasta sitten voidaan oikeasti asettaa vaatimuksia ja valita toimenpiteitä oikeanlaiselle (riittävä, mutta ei ylilyövä) suojaustasolle.

Nollatodennäköisyydellä oleville tapahtumille ei tarvita suojaa, mutta äärimmäisen pieni todennäköisyys pitää usein ottaa huomioon, jos vahingon tai menetyksen arvo (ei välttämättä rahallinen, myös esimerkiksi luottamuksellisuuden menetys) on suuri. Toisaalta, jos tapahtuman todennäköisyys on suuri tai tietyllä aikavälillä varma (esimerkiksi minkä tahansa sähkötoimisen laitteen rikkoutuminen), siihen yleensä pitää varautua, vaikka yhden yksittäisen vahingon vaikutus olisikin pieni.

DIA 34

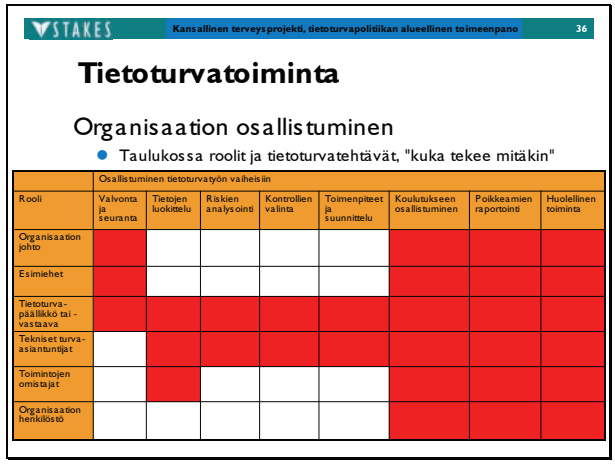


Yksi esimerkki organisaation tietoturvatoiminnan johtamisesta on toteuttaa riskien hallintaan perustuva tietoturvallisuuden hallintajärjestelmä (ISMS) ja käyttää valittuja menettelytapoja hallinnoinnin apuna: tietoturvallisuuskontrollien valinnassa ja toteutuksessa, seurannassa, valvonnassa, raportoinnissa, reagoinnin apuna ja palautteen antamisessa.

Organisoimalla tietoturvallisuustoiminnan sekä dokumentoimalla käytettävät menettelyt organisaation tietoturvatoiminnan voi sertifioida.

”Mitä saa maksaa”: huomaa, että tiedon rahallinen arvo ei välttämättä ole määräävä, vaan tiedon merkitys voi myös olla määräävä tekijä suojaamisvaatimusten määrittelyssä.

DIA 35

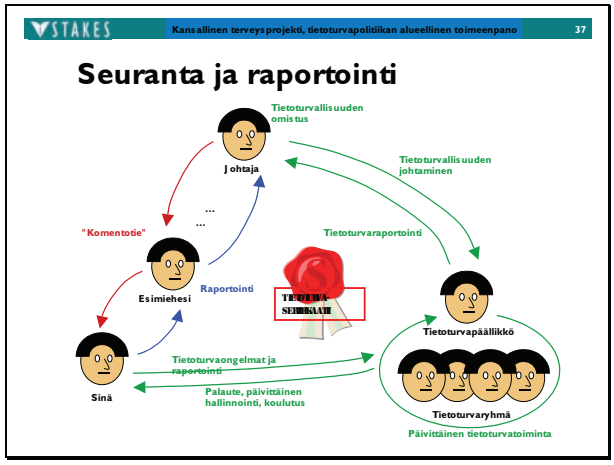


	Osallistuminen tietoturvatyön vaiheisiin							
Rooli	Valvonta ja seuranta	Tietojen luokittelu	Riskien analysointi	Kontrollien valinta	Toimenpiteet ja suunnittelu	Koulutukseen osallistuminen	Poikkeamien raportointi	Huolellinen toiminta
Organisaation johto								
Esimiehet								
Tietoturva-päällikkö tai -vastaava								
Tekniset turva-asiantuntijat								
Toimintojen omistajat								
Organisaation henkilöstö								

Taulukossa näkyvät erilaiset roolit ja organisaation osallistuminen. Huomaa, että organisaation koko henkilöstö on osallisena ja omalta osaltaan vastuussa tietoturvan toteutumisesta noudattamalla omien työtehtäviensä hoidossa huolellisuutta, toteuttamalla raportointivelvollisuuden ja osallistumalla koulutukseen.

Luonnollisesti valvonta, seuranta ja palautteen antaminen kuuluvat myös jokaisen esimiestehtävissä toimivan henkilön velvollisuuksiin.

DIA 36



Kuva on esimerkki tietoturvaorganisaation sovittamisesta linjaorganisaatioon.

Kuvan henkilöt voivat edustaa jokaista organisaation henkilöä. Normaali ”komentotie”, esimies- ja alaissuhteet näkyvät ketjussa Sinä–Esimiehesi–…–Johtaja.

Tietoturvatoiminnan henkilöt ovat oma kokonaisuutensa, ja heidän tuottamansa palvelut ja vastuut on kuvattu vihreillä nuolilla.

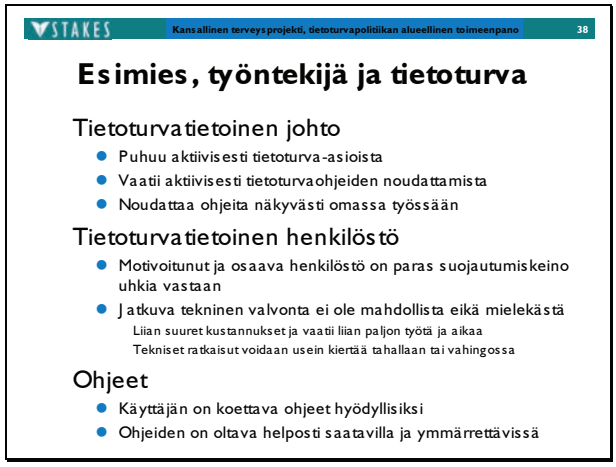
Mallin mukaisesti organisoitu ja dokumentoitu toiminta täyttää tietoturvallisuuden hoidon laatuvaatimukset.

On tärkeää, että tietoturvapäällikkö ja hänen ohjauksessaan toimiva ryhmä on riippumaton ja suoraan ylimmän johdon alaisuudessa eikä esimerkiksi osana tietohallintoa. Näin voidaan taata riippumaton raportointi ja resurssien käyttö turvatoimintaan ja estää mahdolliset eturistiriidat tietohallinnon kanssa. Tietoturvaryhmän jäsenet voivat hallinnollisesti kuulua eri osiin organisaatiota.

Suoraan ylimmän johdon alaisuudessa toimivalle tietoturvaorganisaatiolle voidaan helpommin myöntää tarvittavat oikeudet ja mandaatti toteuttaa valvontatehtäviä koko organisaation laajuisesti.

On myös huomattava, että tietoturvallisuuden osana on myös useita kokonaisuuksia, joilla ei usein ole juuri mitään yhtäläisyyksiä tietohallinnon kanssa. Näitä ovat esimerkiksi henkilöstöhallinto ja kulunvalvonta.

DIA 37



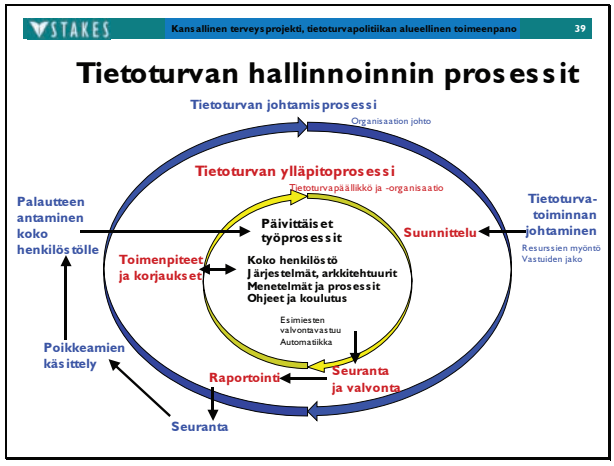
Jos johto kiertää tietoturvamääräyksiä, on varma, että näin tekevät myös työntekijät.

Miksi tietoturvaohjeita ei noudateta?

1. Seuraukset/sanktiot puuttuvat tai eivät ole tiedossa.
2. Sosiaalinen paine, kiire, huolimattomuus ja välinpitämättömyys aikaansaavat laiminlyöntejä ja määräysten rikkomista.
3. Tiedot, taidot ja mahdollisuudet puuttuvat (tekniikka ei toimi, ohjeita ei saatavilla, tekniikka ei riittävän helppokäyttöistä).
4. Tietoturvallisuuden toteuttaminen ja ohjeiden noudattaminen on työn kannalta liian vaivalloista ja tuntuu hyödyttömältä (paljon näkyvillä olevia uhkia, joita vastaan ei suojauduta).

Jos edellä mainitut asiat ovat kunnossa, työntekijälle tulee halu ja aikomus noudattaa ohjeita. Tällöin ohjeita yleensä myös noudatetaan. Kääntäen voi todeta, että jos yksikin edellä mainituista seikoista on puutteellinen, se aikaansaa ohjeiden noudattamatta jättämisen ja tietoturvan laiminlyömisen.

DIA 38



Päivittäiset työprosessit koostuvat organisaation normaalista jokapäiväisestä toiminnasta.

Kuten jo erään aiemman dian yhteydessä todettiin, esimiehen vastuuta ei voi liikaa tähdentää. Se liittyy erittäin oleellisesti päivittäisten työprosessien kulkuun ja noudattamiseen. Esimiehellä on

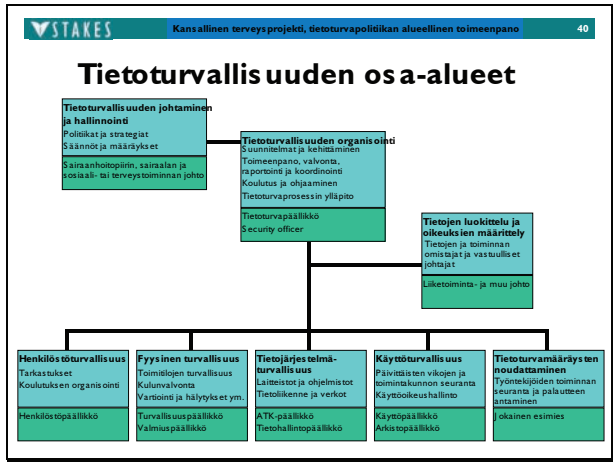
vastuu siitä, että hänen alaisillaan on riittävä osaaminen ja motivaatio tietoturvan huomioimiseen. Esimerkin näyttäminen, valvonta ja palautteen antaminen ovat osa tätä vastuuta. Huomaa, että

- sitouttaminen ei tarkoita pakottamista.
- motivointi ei tarkoita käskemistä.
- koulutus ei tarkoita ulkoa opettelua tai tunnin istumista auditoriossa.
- palautteen antaminen ei ole aina negatiivista eikä koskaan pelkästään negatiivista.

Tietoturvan ylläpitoprosessi on tietoturvapäällikön vastuulla ja hänen tukenaan on riittävä turvaorganisaatio ja tarvittavat resurssit. Prosessi huolehtii henkilöstön koulutuksesta, kontrolli- ja valvontamekanismeista, raportoinnista ja päivittäisistä toimenpiteistä ja korjauksista.

Tietoturvan ylläpitoprosessia ohjaa johtamisprosessi, joka on organisaation johdon vastuulla. Kuvan on tarkoitus selventää kussakin prosessissa suoritettavia toimia ja prosessien välistä tiedon kulkua sekä ohjausta.

DIA 39

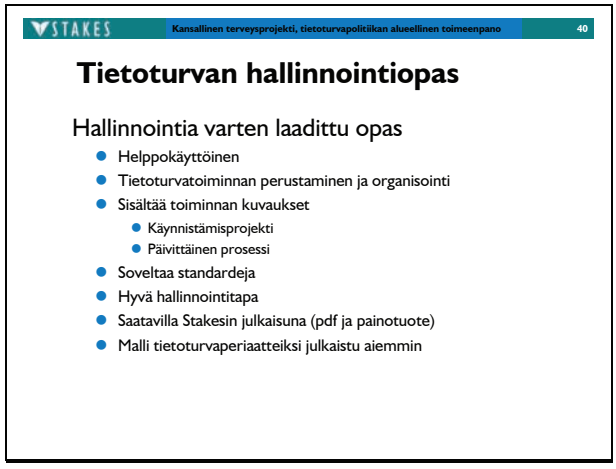


Kaavio on esimerkki tietoturvallisuuden osa-alueista, niiden organisoinnista ja malli tietoturvallisuuteen liittyvien vastuiden ja tehtävien määrittämisestä. Vihertävällä värillä on merkitty se organisaation osa, joka vastaa kyseisen kokonaisuuden tehtävistä.

Kyseinen malli on vain esimerkki: toki muunlainenkin malli on toimiva. Tärkeintä on tunnistaa tarpeelliset vastuut ja tehtävät, sekä henkilöt niitä suorittamaan ja tarpeelliset organisaatiot ja resurssit tukemaan toimintaa.

Esimerkinomainen malli tietoturvan hallinnointiin syntyi osana tietoturvapolitiikan alueellisen toimeenpanon hanketta vuoden 2006 aikana. Malli sisältää oleellisten hallinnointiprosessien kuvauksen ja tehtävät toimijoineen.

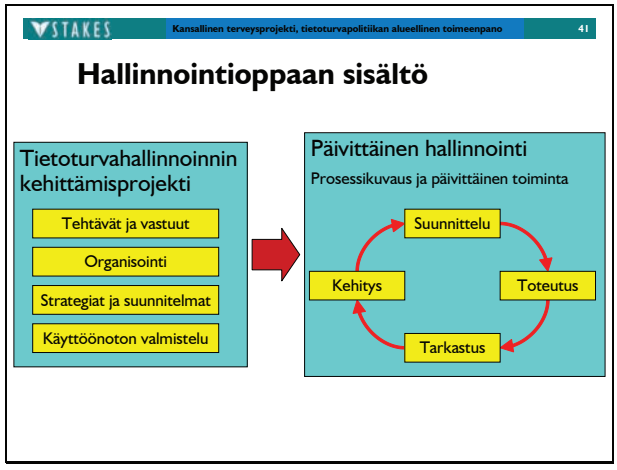
DIA 40



Hallinnointiopas on saatavilla Internetistä (www.stakes.fi/julkaisut) tai painettuna (Stakes).

Myös aiemmin julkaistut tietoturvaperiaatteet on saatavilla verkosta tai painettuna.

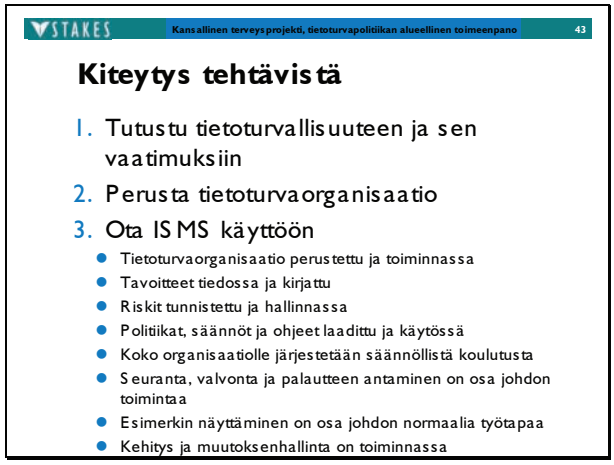
DIA 41



Hallinnoinnin kehittämisprojektissa määritetään tietoturvahallinnoinnin tehtävät ja vastuut, sovitaan niiden tekijästä (esimerkiksi tietoturvapäällikkö tai tietoturvavastaava), laaditaan tarvittavat strategiat ja suunnitelmat sekä valmistellaan käyttöönotto (mm. määritellään resurssit, hallinnoinnin prosessi ja päivittäiset toimenpiteet seurantoineen).

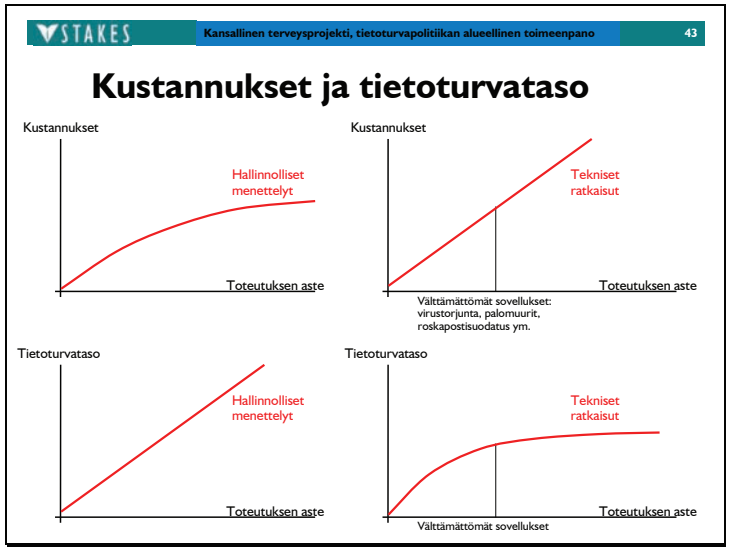
Päivittäinen hallinnointi sisältää kaikki jatkuvan syklisen prosessin vaiheet ja toiminnot.

DIA 42



Kohta 2: oppaan osiot 1 ja 2.
Kohta 3: oppaan osio 3 kuvaa päivittäisen toiminnan.

DIA 43



Kahdessa ylemmässä käyrässä näkyy toteutusten ja kustannusten välinen suhde: hallinnollisten menettelyiden kustannukset eivät tiettyjen perusinvestointien jälkeen nouse samalla tavalla kuin teknisistä ratkaisuista aiheutuvat kustannukset. Välttämättömiin teknisiin ratkaisuihin sisältyvät myös muuten kuin tietoturvabudjetista rahoitettavat ratkaisut, esimerkiksi kulunvalvonta ja henkilökortit.

Kahdessa alemmassa käyrässä näkyy puolestaan hallinnollisten ja teknisten menettelyjen määrän nostamisen vaikutus tietoturvatasoon. Hallinnollisten menettelyjen lisääminen parantaa tietoturvaa paremmin kuin teknisten määrittelyjen lisääminen.

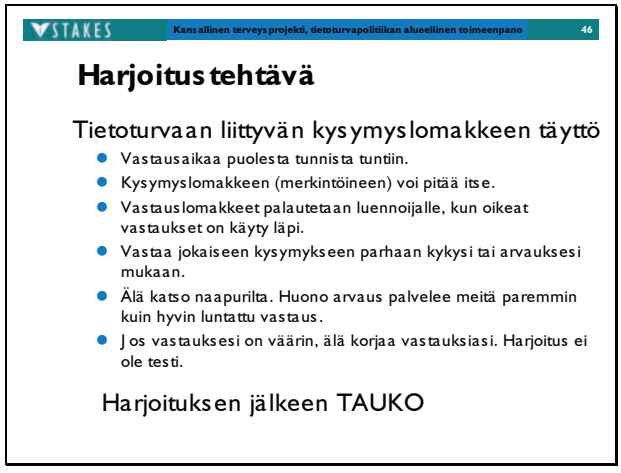
DIA 44

Koulutus lähenee loppuaan ja vuorossa on harjoitustehtävä.

Johdon materiaali: harjoitus tehdään yhteisenä keskusteluna.

Organisaation henkilöstön materiaali: käytä kysymyslomaketta, jonka perusteella täytetään vastauslomake. Esitysmateriaalissa käydään läpi kyselyn oikeat vastaukset.

DIA 45

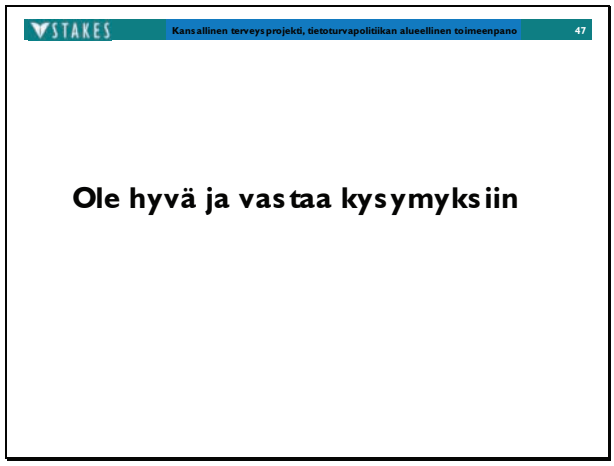


Osallistujille on kerrottava, että harjoitus ei ole testi tai koe.

Harjoituksen jälkeen pidetään 10–20 minuutin tauko. Jokaiselle annetaan riittävästi aikaa, että kaikkiin kysymyksiin ehditään vastaamaan.

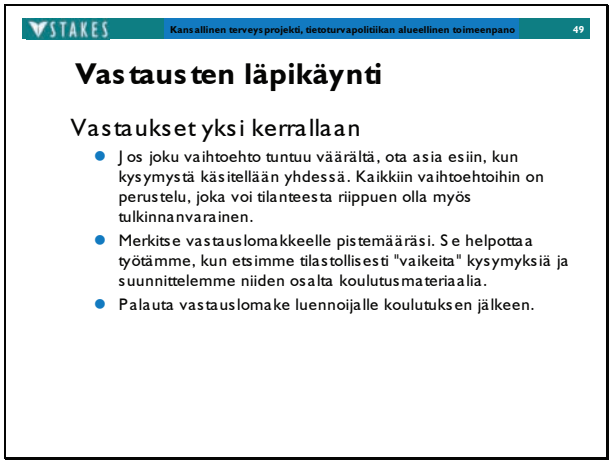
Osallistujat voivat tehdä kysymyslomakkeelle omia merkintöjäsi, sillä kysymyslomaketta ei tarvitse palauttaa. Hyvä tapa täyttää vastauslomake on vastata ensin kaikkiin kysymyksiin kysymyslomakkeelle, ja vasta sen jälkeen täyttää vastauslomake.

DIA 46



DIA 47

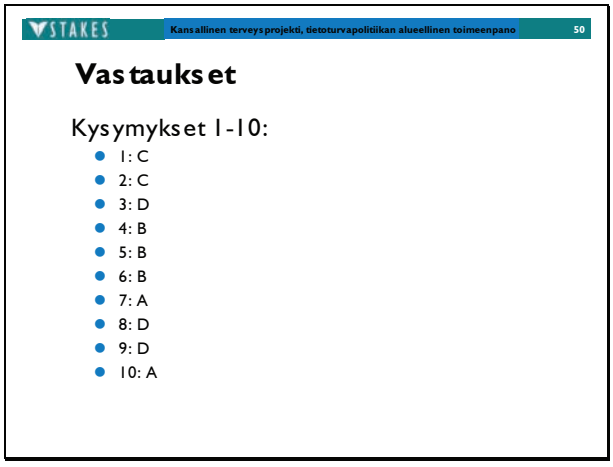
DIA 48



Vastauslomakkeet palautetaan nimettömänä ja tuloksia käytetään ainoastaan tilastointiin ja koulutusmateriaalin kehittämiseen.

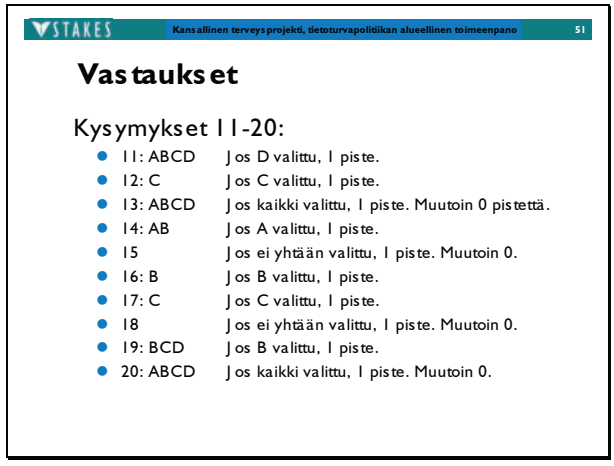
Ainoastaan oikeat vastaukset ovat esillä seuraavilla dioilla. Perustelut ovat luennoijan materiaalissa. On otettava huomioon, että kysymyksiin ei ole välttämättä olemassa vain yhtä oikeaa vastausta, joten keskustelu on sallittua ja toivottavaa.

DIA 49



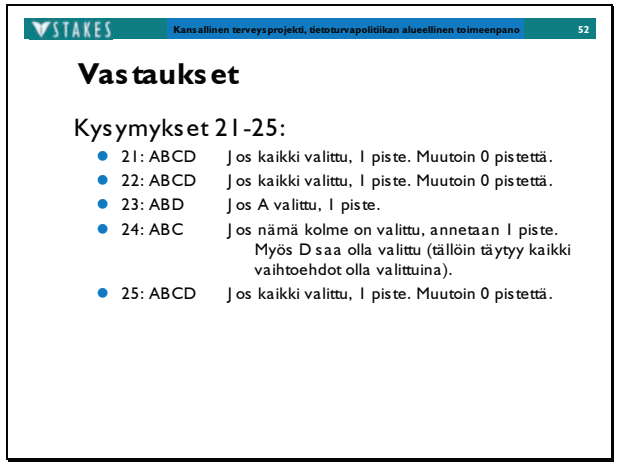
Käytä luennoijan materiaalia perusteluiden esittelyssä.
Esitetyistä vastauksista kustakin yksi piste, muutoin ei pisteitä.

DIA 50



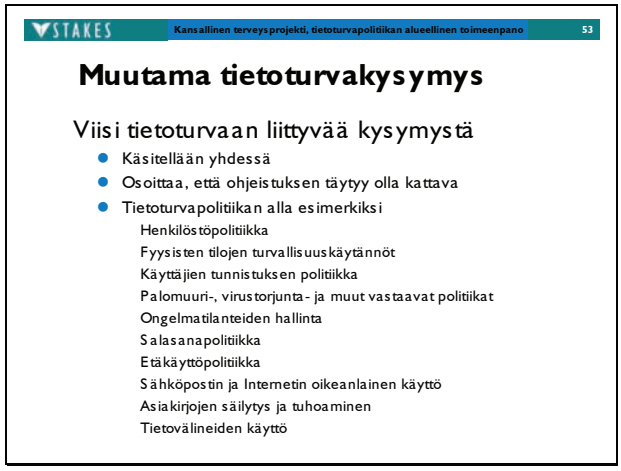
Käytä luennoijan materiaalia perusteluiden esittelyssä.

DIA 51



Käytä luennoijan materiaalia perusteluiden esittelyssä.

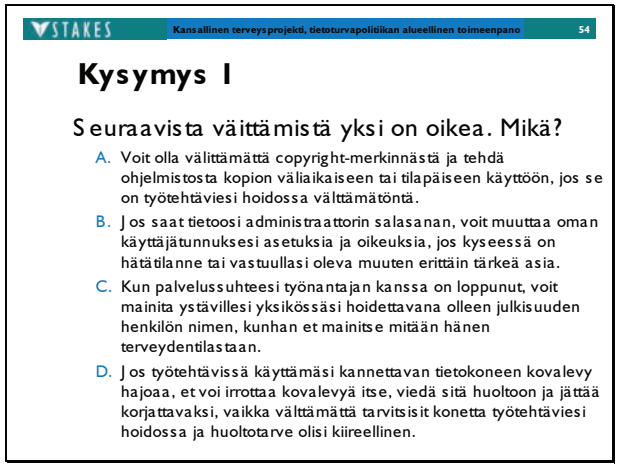
DIA 52



Ohjeistukset ja politiikat ovat laaja kokonaisuus, josta tässä on mainittu muutama esimerkki.

Tehtyjen kyselyiden perusteella esimerkiksi mainittuihin kysymyksiin on tullut erilaisia vastauksia myös asiantuntijatasolla. Seuraavassa viisi esimerkkiä kysymyksistä.

DIA 53

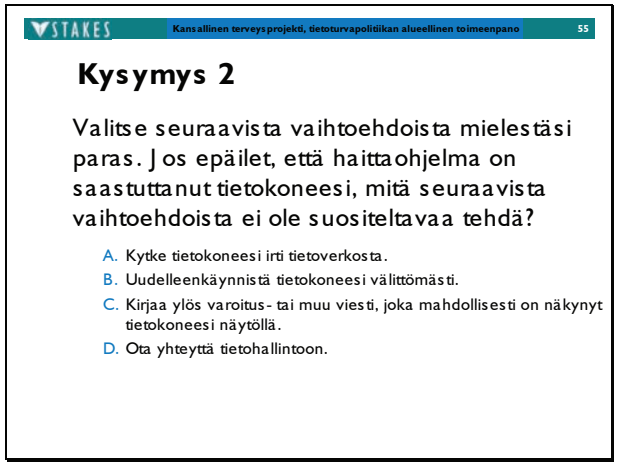


Esitetyistä vaihtoehdoista oikea on kohta D.

Kovalevyllä saattaa olla arkaluonteista tietoa esimerkiksi välimuistitiedostoissa, vaikkeivät ohjelmistot tai tietokannat olisikaan kannettavassa tietokoneessa.

Kohta A: luvaton kopiointi on aina rikos eikä sitä voi perustella tarpeella. Myös kohta B voidaan tulkita laittomaksi ja pahimmassa tapauksessa tietomurroksi. Kohta C: luottamuksellisuus ja salassapito koskevat myös työsuhteen loppumisen jälkeistä aikaa.

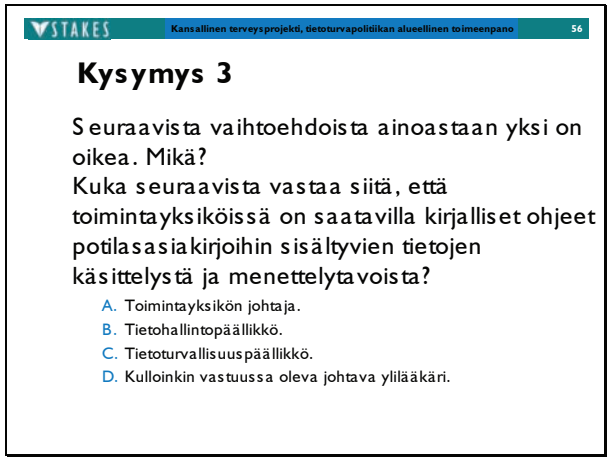
DIA 54



Esitetyistä vaihtoehdoista oikea on kohta B, siis tietokonetta ei ole syytä uudelleenkäynnistää. Jos tietokone on jo saastunut, ei uudelleenkäynnistys auta mitään. Päinvastoin: jotkut haittaohjelmat saattavat saada käynnistyksessä uutta ”puhtia” ja saada aikaan muita haittavaikutuksia. Haittaohjelma saattaa esimerkiksi aktivoitua tekemään erilaisia tuhoamis- tai muutostoimia tietokoneen tiedostoihin tai määrityksiin, jonka jälkeen torjuntatyö saattaa olla jopa mahdotonta.

Jos epäilee tietokoneensa olevan haittaohjelman saastuttama, on syytä kytkeä kone irti tietoverkosta estääkseen mahdollisen tartunnan leviämisen. Jotta tilanteen selvitys olisi mahdollisimman tehokasta, kaikki virheilmoitukset on syytä kirjata ylös mahdollisuuksien mukaan. Yhteydenotto tietohallintoon tai tietoturvayksikköön aloittaa mahdollisen ongelman selvittämisen.

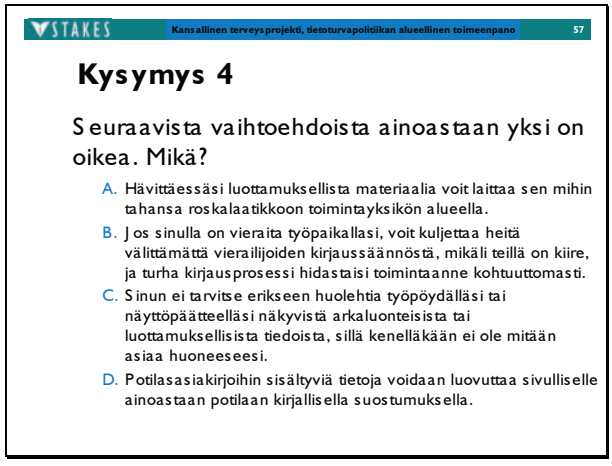
DIA 55



Esitetyistä vaihtoehdoista oikea on kohta A. Sosiaali- ja terveysministeriön asetuksessa potilasasiakirjojen laatimisesta ja säilyttämisestä todetaan toimintayksikön johtajan toimivan rekisterinpitäjän edustajana. Tätä vastuuta toimintayksikön johtaja ei voi sopimuksellisesti tai itse toisin määräämällä siirtää organisaatiossaan toisaalle.

Edellä mainitun perusteella kohdat B, C ja D ovat väärin eikä lisäperusteluja kaivattane. Käytännön ohjeistuksen laatimisen ja jakelun toimintayksikön johtaja on toki luultavasti vastuuttanut organisaatiossaan sopivalle taholle, mutta lakisääteinen vastuu ei tällä toimenpiteellä siirry.

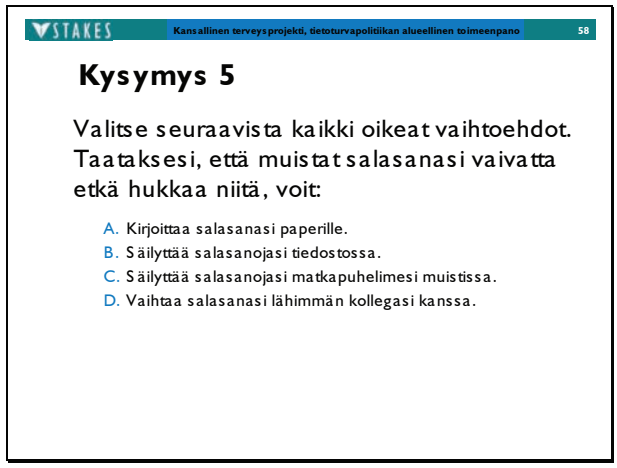
DIA 56



Esitetyistä vaihtoehdoista oikea on kohta D. On huomattava, että tietyissä erityistilanteissa ja tietyille sivullisille tahoille (kuten Kela, poliisiviranomainen, kunnallinen sosiaaliviranomainen) tietoja luovutettaessa ei välttämättä tarvita potilaan kirjallista lupaa. Nämä tilanteet ilmenevät laissa potilaan asemasta ja oikeuksista.

Kohta A on väärin, mutta jos organisaatiossa ei ole varattu luottamuksellista ja arkaluonteista materiaalia varten asianmukaista tuhoamismenettelyä (silppurit, tietoturvaroskikset ym.), tämä voi aiheuttaa vääriä vastauksia. Kohta B on selkeästi väärin riippumatta mahdollisesta kiireestä tai muista olosuhteista. Jos kyseessä on hätätilanne, esimerkiksi evakuointi, ei esimerkiksi uloskirjausta tietenkään tarvita, jos se voi vaarantaa ihmisten terveyden tai fyysisen turvallisuuden. Kohta C on yksiselitteisesti väärin: luottamuksellista tietoa on käsiteltävä asianmukaista huolellisuutta ja salassapitosäännöksiä noudattaen. Näyttöpäätteelle jättäminen ei noudata hyvää tiedonhallintatapaa missään tiloissa.

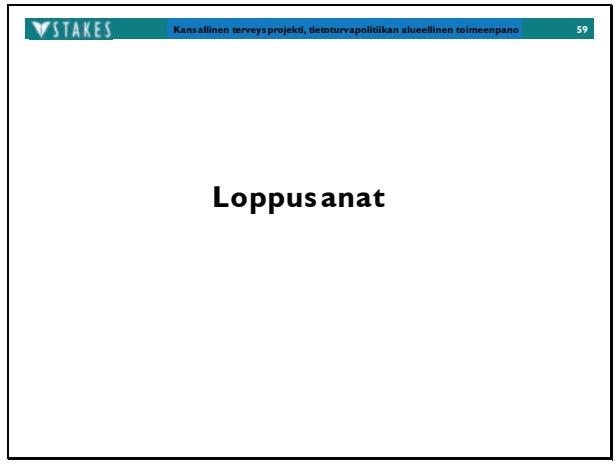
DIA 57



Esitetyistä vaihtoehdoista kaikki ovat väärin.

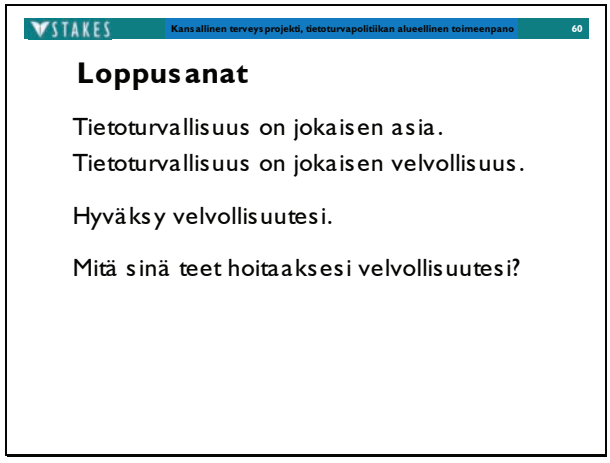
Nämä ovat kuitenkin sääntöjä, joita vastaan usein rikotaan. On ensiarvoisen tärkeää saada tietojärjestelmien käyttäjät havaitsemaan uhkat. Jos ulkopuolinen pääsee heidän tunnuksillaan tietojärjestelmään, myös henkilön oma oikeusturva on kyseessä. On muistettava, että henkilön käyttäjätunnus ja salasana == henkilö itse. Henkilö vastaa siitä, että salasana on sellainen, että vain hän itse sen tietää ja muilla ei sitä ole mahdollisuutta selvittää. Kohta B voi tuottaa hiuksen halkomista. Tietojärjestelmissähän salasanoja säilytetään nimenomaan järjestelmän sisäisessä tiedostossa, tosin kryptatussa muodossa.

DIA 58



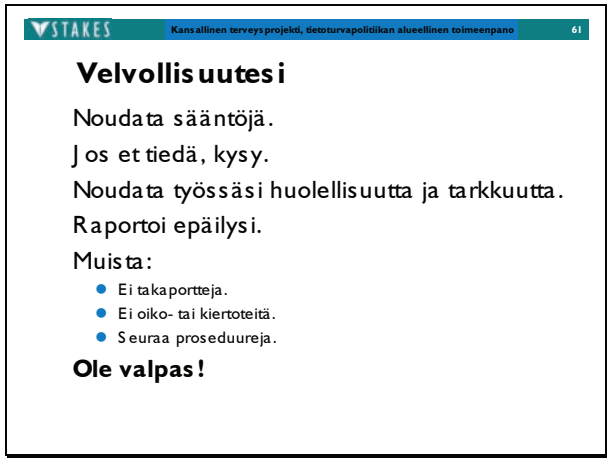
Vielä loppusanat.

DIA 59



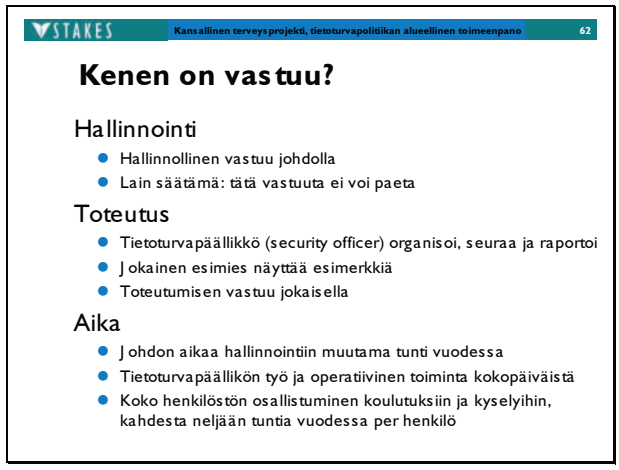
Jo esitetyn kertausta.

DIA 60



Tämäkin on käyty läpi jo aiemmin: jos ei tiedä, jos ei osaa tai jos on pienikin epäilys, on parempi kysyä kuin tehdä ja katua myöhemmin.

DIA 61



Kertauksen vuoksi:

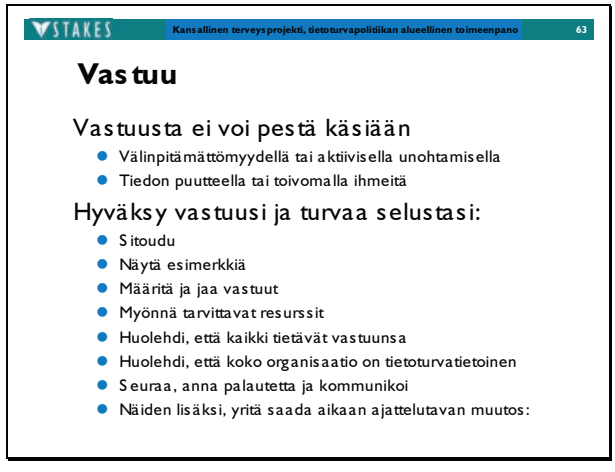
Johtaminen alkaa vastuiden hyväksymisestä. Sillä aloitetaan tietoturvakulttuurin luominen koko organisaatioon.

Johtamalla tietoturvaa, valtuuttamalla tietoturvatoiminnan käytännön organisointi nimetylle tietoturvapäällikölle, myöntämällä tarvittavat resurssit ja seuraamalla tietoturvapäällikön raportointia ja valvomalla täten koko organisaation toimintaa johto voi luoda aukottoman tietoturvan hallintajärjestelmän (ISMS, kuten edellisessä diassa kuvattiin).

Tietoturvaryhmä voi koostua eri yksiköiden henkilöistä, jotka hoitavat tietoturvatöitä oman asiantuntemuksensa puitteissa tarpeen mukaan.

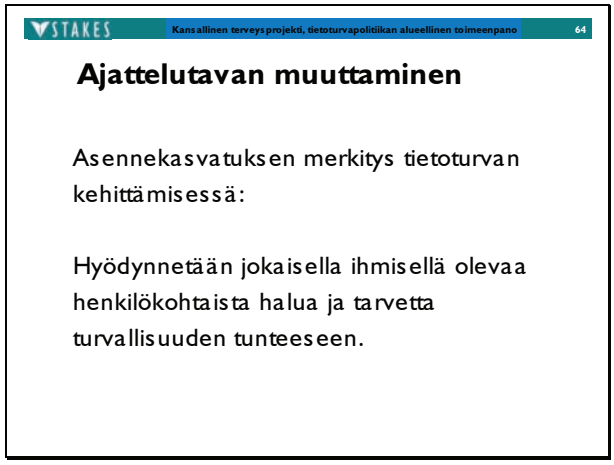
Työntekijöiden jokapäiväisen työn ohjaus ja valvonta kuuluvat normaaleihin esimiesvelvollisuuksiin, johon tietoturvallisuus ei tee poikkeusta. Siksi esimiesten rooli esimerkin näyttäjänä ja palautteen antajana on tärkeä ja se pitää jokaisen esimiehen myös tiedostaa.

DIA 62



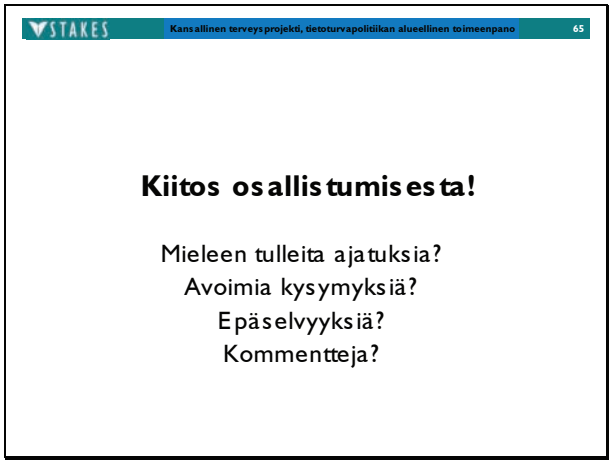
Ellei sitoutumista ole ja ellei toimia ole jo käynnistetty, on syytä sitoutua ja kannattaa käynnistää järjestelyt heti. On turha odottaa.

DIA 63



Ihmisellä on henkilökohtainen halu turvallisuuden ja hyvinvoinnin tunteeseen, sitä hyödyntämällä tietoturvallisuuden toteutuminen ja parantaminen on mahdollista saavuttaa kohtuullisilla resursseilla ja kustannuksilla.

DIA 64

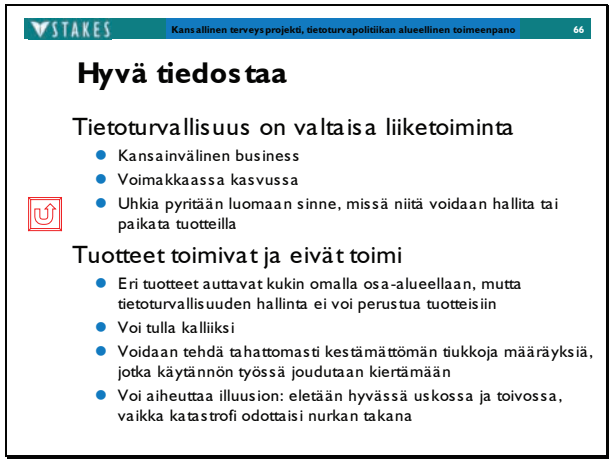


Loppukeskustelu ja avointen kysymysten käsittely. Myös termistöä voidaan käsitellä kysymysten yhteydessä.

Kannattaa myös kysyä, vastasivatko koulutus ja aiheet sitä, mitä kuulijat odottivat.

Lisädiat muistiinpanoineen

DIA 65



Tietoturvatuotteita myydään, ja niitä voi toki ostaa, ja on pakkokin ostaa. Mutta sillä ei vielä osteta turvallisuutta. Se saavutetaan johtamisella, hallinnoinnilla, organisoinnilla ja kouluttamalla.

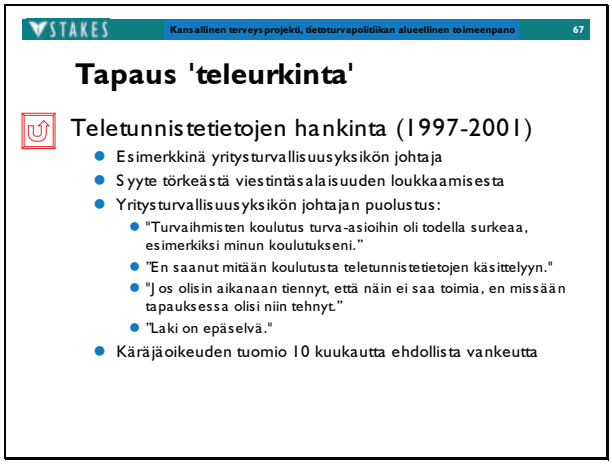
Tietoturvallisuutta myydään jopa ”ulkoistamalla”. Tällöin tarkoitetaan yleensä verkkoturvallisuuden teknisiä menettelyitä (palomuurit, virustorjunta, valvonta ja hälytykset sekä korjaukset). Organisaation turvallisuuden johtamista ei käytännössä voi (eikä kannatakaan) ulkoistaa, sillä johto on joka tapauksessa vastuussa.

Yksi esimerkki liian tiukoista määräyksistä on luottamuksellisen materiaalin poisto turvaroskakoriin, jollaista ei välttämättä ole saatavilla. Tämä johtaa määräyksen laiminlyöntiin.

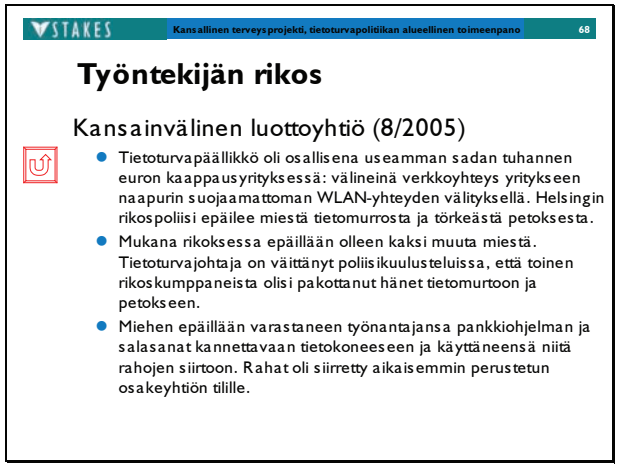
Esimerkki liian tiukasta teknisesti toteutetusta säännöstä on kaikkien sähköpostin kuvaliitetiedostojen suodatus, jolloin politiikka estää myös aiheellisten kuvatiedostojen lähetyksen/vastaanottamisen (röntgenkuvat, magneettikuvat, ym.).

Myynti uhkakuvien avulla on perinteinen keino myydä tietoturvallisuutta ja sen suojelemiseksi tarkoitettuja tuotteita. Tuotteita on myyty runsaasti, ja myynti on yhä kasvussa. Kysymys ”onko tietoturvallisuuden taso noussut?” on tarpeellinen, mutta vastaus voi olla vaikea löytää.

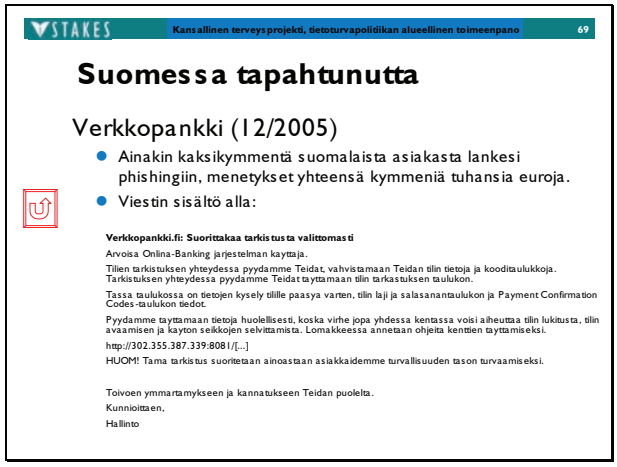
DIA 66



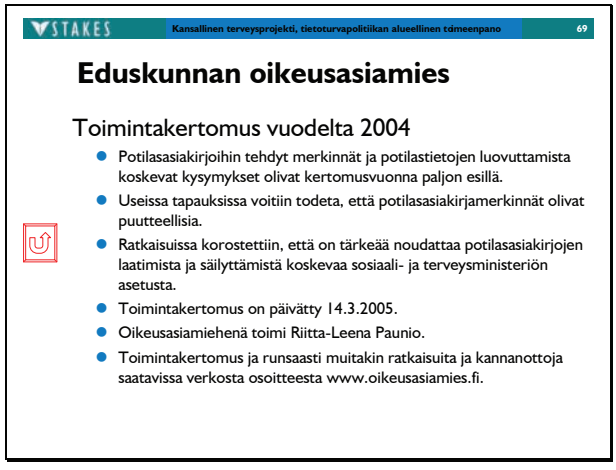
DIA 67



DIA 68



DIA 69

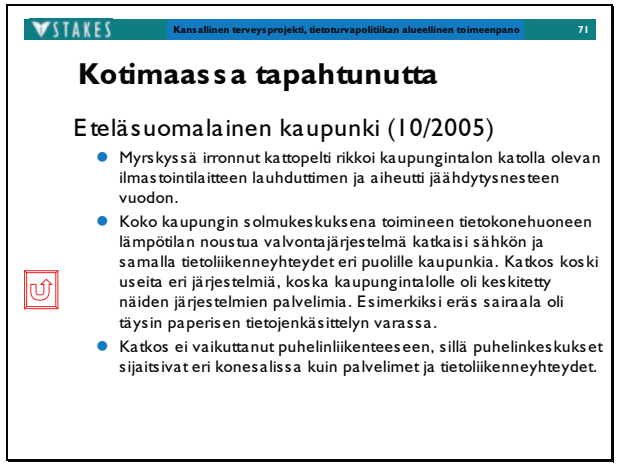


Ratkaisut koskivat muun muassa seuraavia tapauksia:

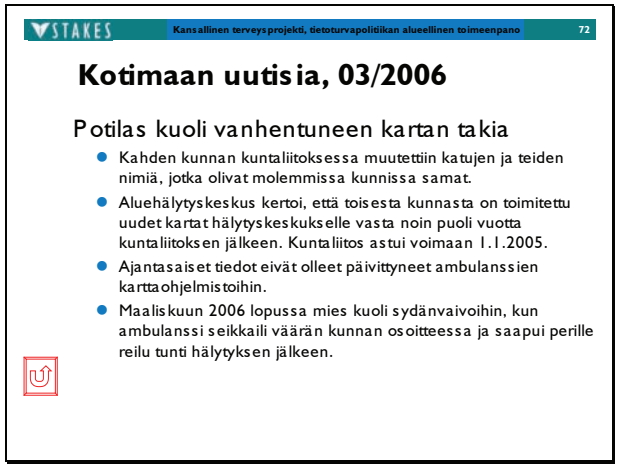
- Toimenpiteen lainmukaisuuden on oltava vaikeuksitta arvioitavissa potilasasiakirjojen perusteella.

- Potilasasiakirjoihin on merkittävä potilaan oma kanta (suonensisäinen lääkitys).
- Jos uskonnollinen vakaumus on merkitty potilasasiakirjoihin, on toimittu virheellisesti.
- Hoitajien muistiinpanot kuuluvat potilasasiakirjoihin, ylilääkärin olisi tullut antaa potilaan edustajalle hänen pyytämänsä jäljennökset.
- Rekisteröidyn tarkastuspyyntöä henkilötietolain edellyttämällä tavalla ei oltu toteutettu ilman aiheetonta viivytystä. Rekisterinpitäjällä ei ole harkintavaltaa sen suhteen, kuinka usein rekisteröity saa käyttää tarkastusoikeuttaan.

DIA 70

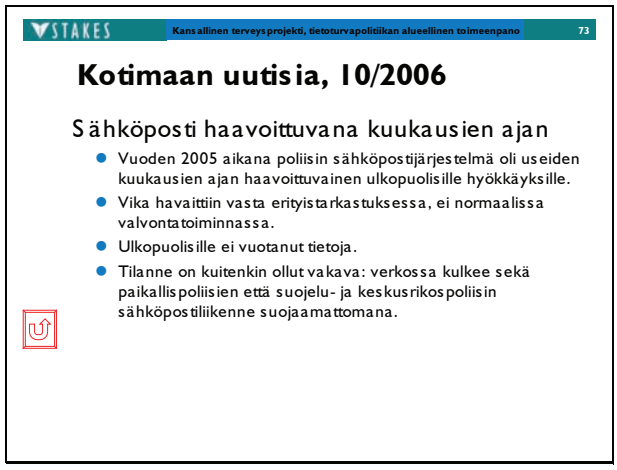


DIA 71



Valitettavasti vastaavia tapauksia on esillä julkisuudessa säännöllisesti. Vaikka päivystys-, hälytys-, kuljetus- ja hoitoprosessit olisivat kuinka tehokkaiksi hiottu, ei tämä välttämättä riitä, jos prosesseissa tarvittavat tiedot eivät ole käytettävissä tai oikeellisia.

DIA 72


STAKES
Kansallinen terveysprojekti, tietoturvapolitiikan alueellinen toimeenpano
73
Kotimaan uutisia, 10/2006
Sähköposti haavoittuvana kuukausien ajan
Vuoden 2005 aikana poliisin sähköpostijärjestelmä oli useiden kuukausien ajan haavoittuvainen ulkopuolisille hyökkäyksille.
Vika havaittiin vasta erityistarkastuksessa, ei normaalissa valvontatoiminnassa.
Ulkopuolisille ei vuotanut tietoja.
Tilanne on kuitenkin ollut vakava: verkossa kulkee sekä paikallispoliisien että suojelu- ja keskusrikospoliisin sähköpostiliikenne suojaamattomana.

Tietoturvakoulutuksen kysymys- ja vastauslomakkeet ohjeineen

Kysymyslomake

Ohjeita

Tämä kysely ei ole testi. Sitä käytetään ainoastaan harjoituksena, osana tietoturvallisuuskoulutusta, ja sen tarkoitus on auttaa Sinua havaitsemaan tietoturvallisuuteen ja tietosuojaan liittyviä asioita jokapäiväisessä työssäsi. Kysely auttaa meitä kehittämään koulutuksen laatua ja valitsemaan koulutusohjelmaan parhaiten sopivat aiheet ja yksityiskohdat. Voit tehdä tähän kysymyslomakkeeseen omia merkintöjäsi, sillä saat pitää lomakkeen itselläsi koulutuksen jälkeen oman muistisi virkistämiseksi. Kaikki kommentit ja mielipiteet ovat tervetulleita, kun käsittelemme lopuksi vastausvaihtoehtoja ja niiden oikeellisuutta. Rohkaisemme kaikkia osallistumaan keskusteluun ja esittämään omat näkemyksensä.

Aikaa kuhunkin vastaukseen on käytettävissä vain hieman yli minuutti, joten älä juutu yhteen kysymykseen. Jotta vastaukset tuottavat meille tarpeellisen tiedon koulutuksen kehittämisessä, tarvitsemme kaikilta vastaukset myös viimeisiin kysymyksiin. Vastausaikaa voidaan tarvittaessa pidentää, jotta kaikki ehtivät vastaamaan jokaiseen kysymykseen. Aihepiiri on joillekin erittäin tuttu, mutta se voi olla toisille melko tuntematon, joten jotkut saattavat selviytyä testistä huomattavan nopeasti. Tästä syystä pidämme lyhyen tauon, kun vastauslomakkeet on täytetty. Palauta lomake vasta tauon jälkeen, kun olemme käsitelleet oikeat vaihtoehdot, jos haluat selvittää omat pisteesi.

Vastaa kysymyksiin erilliselle vastauslomakkeelle. Vaikka et tietäisi vastauksia, valitse vastausvaihtoehdoista paras tai parhaat arvauksesi. Koska kyseessä ei ole testi, meidän kannaltamme myös väärät vastaukset ovat oikeita, sillä ne auttavat meitä kehittämään koulutusohjelmaa oikeaan suuntaan. Siksi pyydämme, että olet rehellinen valitessasi oikeita vastauksia. Älä korjaa vastauksiasi jälkikäteen. Keräämme vastauslomakkeet esitettyämme oikeat vastaukset. Pyydämme palauttamaan vastauslomakkeen nimettömänä luennoijalle. Lomaketta käytetään ainoastaan koulutuksen laadun kehittämisessä ja tietoturvallisuusosaamiseen liittyvässä tilastoinnissa. Halutessasi voit jättää pisteesi laskematta. Pistelasku on mukana vain oman mielenkiintosi herättämiseksi.

Kysely liittyy ainoastaan tietoturvallisuuskoulutukseen, eikä sitä saa käyttää muissa yhteyksissä tai osana vastaajien testausta missään testissä tai kokeessa. Kysymykset ja vastausvaihtoehdot on valittu siten, että ne palvelevat nimenomaan koulutustarkoituksessa ja Stakesin suunnitteleman koulutuskokonaisuuden yhteydessä. Jos haluat käyttää kysymyksiä jossakin muussa yhteydessä, ota Stakesiin etukäteen yhteyttä.

Kaikissa kysymyksissä tarkoitetaan työympäristössä toimimista (työsähköposti, Internetkäyttö työpaikalta, ym.) ellei toisin nimenomaisesti mainita.

Ensimmäinen kysymysosio

Kunkin seuraavan kysymyksen vastaukseksi sopii esitetyistä vaihtoehdoista täsmälleen yksi, joka on joko ainoa täysin oikea tai sellainen, joka parhaiten kuvaa lähinnä olevaa oikeaa vaihtoehtoa. Valitse siis kuhunkin kysymykseen neljästä vastausvaihtoehdosta yksi.

Kysymys 1
Mikä seuraavista vaihtoehdoista kuvaa parhaiten sitä tahoa, jolle voit kertoa havaitsemastasi tai epäilemästäsi tietoturvaongelmasta?

A) Sanomalehti, televisio tai muu media.
B) Poliisiviranomainen.
C) Organisaatiosi tietoturvallisuuspäällikkö.
D) Lähin kollegasi.

Kysymys 2
Mikä seuraavista on vähimmäisvaatimus hyvälle salasanalle?

A) Kaikki salasanat ovat hyviä, eikä vähimmäisvaatimusta ole.
B) Vähintään viisi merkkiä pitkä.
C) Vähintään kymmenen merkkiä pitkä, joista yhden täytyy olla numero tai erikoismerkki.
D) Vähintään viisitoista merkkiä pitkä, joista vähintään yhden täytyy olla numero ja vähintään yhden erikoismerkki.

Kysymys 3
Seuraavista väittämistä ainoastaan yksi on oikea. Mikä?

A) Voit olla välittämättä copyright-merkinnästä ja tehdä ohjelmistosta kopion väliaikaiseen tai tilapäiseen käyttöön, jos se on työtehtäviesi hoidossa välttämätöntä.
B) Jos saat tietoosi administraattorin salasanan, voit muuttaa oman käyttäjätunnuksesi asetuksia ja oikeuksia silloin, kun kyseessä on hätätilanne tai muutoin erittäin tärkeä asia, josta sinun täytyy huolehtia.
C) Kun palvelussuhteesi työnantajan kanssa on loppunut, voit mainita ystävillesi yksikössäsi hoidettavana olleen julkisuuden henkilön nimen, kunhan et mainitse mitään hänen terveydentilastaan.
D) Jos työtehtävissä käyttämäsi kannettavan tietokoneen kovalevy hajoaa, et voi irrottaa kovalevyä itse, viedä sitä huoltoon ja jättää korjattavaksi, vaikka välttämättä tarvitsisit konetta työtehtäviesi hoidossa ja huoltotarve olisi kiireellinen.

Kysymys 4
Seuraavista väittämistä ainoastaan yksi on oikea. Mikä?

A) Voit liittää kollegasi sähköpostiosoitteen ainoastaan sellaiselle postituslistalle, jossa käsitellään asioita, jotka auttavat kollegaasi hänen työtehtäviensä hoidossa.
B) Voit tallettaa sähköpostissa saamasi liitetiedoston oman tietokoneesi kovalevylle.
C) Suojellaksesi lähettämiesi viestien luottamuksellisuutta voit ottaa käyttöösi salausohjelmiston ja luoda oman avainparin, jonka avulla voit salata kaikki lähettämäsi viestit.
D) Voit vaihtaa henkilökohtaisen käyttäjätunnuksesi ja salasanasi lähimmän kollegasi kanssa hänen vastaavaan tunnukseensa ja salasanaansa, jos voitte näin toimia toistenne varahenkilöinä tai tästä vaihdosta on teille muuten apua työtehtävienne hoidossa.

Kysymys 5

Seuraavista väittämistä ainoastaan yksi on oikea. Mikä?

A) Voit lähettää sähköpostilla liitetiedostoja välittämättä niiden koosta, koska vastaanottajan sähköpostijärjestelmä huolehtii liian suurien tai mahdollisesti muuten sopimattomien liitetiedostojen oikeanlaisesta käsittelystä.
B) Sähköpostiohjelmistoissa löytyy ominaisuus, jonka avulla voit lähettää sähköpostiviestin useille henkilöille yhtaikaa ilman, että vastaanottajat näkevät toistensa sähköpostiosoitteita.
C) Jos vastaanotat viruksesta varoittavan viestin esimerkiksi sähköpostitse, se kannattaa lähettää eteenpäin mahdollisimman monelle kollegallesi ja muille tuttavillesi.
D) Voit pitää tai tallettaa rajoittamattoman määrän vastaanottamiasi sähköpostiviestejä sähköpostipalvelimella välittämättä niiden mahdollisesti viemästä levytilasta, sillä sama levytila kuluu tallennettaessa viestit ja liitetiedostot esimerkiksi verkkolevylle.

Kysymys 6

Valitse seuraavista vaihtoehdoista mielestäsi paras. Jos epäilet, että haittaohjelma on saastuttanut tietokoneesi, mitä seuraavista vaihtoehdoista **ei** ole suositeltavaa tehdä?

A) Kytke tietokoneesi irti tietoverkosta.
B) Uudelleenkäynnistä tietokoneesi välittömästi.
C) Kirjaa ylös varoitus- tai muu viesti, joka mahdollisesti on näkynyt tietokoneesi näytöllä.
D) Ota yhteyttä tietohallintoon.

Kysymys 7

Seuraavista vaihtoehdoista ainoastaan yksi on oikea. Mikä?

Kuka seuraavista vastaa siitä, että toimintayksiköissä on saatavilla kirjalliset ohjeet potilasasiakirjoihin sisältyvien tietojen käsittelystä ja menettelytavoista?

A) Toimintayksikön terveydenhuollosta vastaava johtaja.
B) Toimintayksikön tietohallintopäällikkö.
C) Toimintayksikköön nimetty tietoturvallisuuspäällikkö.
D) Kulloinkin vastuussa oleva johtava ylilääkäri.

Kysymys 8

Seuraavista väittämistä ainoastaan yksi on oikea. Mikä?

A) Hävittäessäsi luottamuksellista materiaalia voit laittaa sen mihin tahansa roskalaatikkoon toimintayksikön alueella.
B) Jos sinulla on vieraita työpaikallasi, voit kuljettaa heitä välittämättä vierailijoiden kirjaussäännöstä, mikäli teillä on kiire, ja turha kirjausprosessi hidastaisi toimintaanne kohtuuttomasti.
C) Sinun ei tarvitse erikseen huolehtia työpöydälläsi tai näyttöpäätteelläsi näkyvistä arkaluonteisista tai luottamuksellisista tiedoista, sillä kenelläkään ei ole mitään asiaa huoneeseesi.
D) Potilasasiakirjoihin sisältyviä tietoja voidaan luovuttaa sivulliselle ainoastaan potilaan kirjallisella suostumuksella.

Kysymys 9
Seuraavista vaihtoehdoista ainoastaan yksi on oikea. Mikä?
Potilasasiakirjojen, näytteiden ja mallien säilytys sosiaali- ja terveysministeriön asetuksella säädetyn säilytysajan päätyttyä:

A) On ehdottomasti kiellettyä, ja ne on aina hävitettävä asetuksen mukaisesti.
B) On mahdollista Arkistolaitoksen luvalla.
C) On mahdollista toimintayksikön tietohallintopäällikön luvalla.
D) On mahdollista, jos se on välttämätöntä potilaan hoidon takia.

Kysymys 10
Seuraavista vaihtoehdoista ainoastaan yksi on oikea. Mikä?
Terveydenhuollon ammattihenkilön sanelun perusteella tehtyjen merkintöjen oikeellisuudesta vastaa:

A) Sanelija.
B) Merkintöjen tekijä.
C) Tietohallintoyksikkö, jos se on antanut käyttöön välineet merkintöjen tekemiseksi sanelun perusteella.
D) Kulloinkin vastuussa oleva johtava ylilääkäri.

Toinen kysymysosio

Kussakin seuraavassa kysymyksessä vastaukseksi sopii esitetyistä vaihtoehdoista mikä tahansa määrä vastauksia (0–4 oikeaa vastausta). Huomaa siis, että tietyn kysymyksen vaihtoehdot voivat kaikki olla vääriä tai vastaavasti myös oikeita. Valitse kuhunkin kysymykseen kaikki mielestäsi kelpaavat vaihtoehdot.

Nähtyäsi oikeat vastaukset ja ollessasi sitä mieltä, että joku luennoijan oikeaksi esittämistä vaihtoehdoista on väärä tai vääräksi esittämistä vaihtoehdoista oikea, pyydämme Sinua ehdottomasti tuomaan asian esiin. Jokaiselle vaihtoehdolle on selkeä perustelu, miksi kyseinen vaihtoehto on joko väärä tai oikea.

Kysymys 11
Valitse seuraavista kaikki oikeat vaihtoehdot.
Kuka on vastuussa tietoturvan toteutumisesta toimintayksikössäsi?

A) Toimintayksikön johtaja.
B) Kaikki esimiesasemassa olevat.
C) Tietohallintoyksikkö.
D) Jokainen työntekijä.

Kysymys 12
Valitse seuraavista tietoturvapolitiikkaa koskevista väitteistä kaikki oikeat.

A) Tietoturvapolitiikka on tietohallintoyksikön käyttöön tarkoitettu ohje, joka sisältää hyviä ajatuksia tietoturvallisuuden kehittämisestä ja jonka avulla ylläpidetään tietoturvallisuutta terveydenhuollon eri toimintayksiköissä.
B) Tietoturvapolitiikka sisältää päivittäisiä tietoturvaohjeita järjestelmien vastuuhenkilöille.
C) Tietoturvapolitiikka on toimintayksikön johdon hyväksymä ja koko toimintayksikön laajuisesti käyttöön määräämä.
D) Voit jättää tietoturvapolitiikan huomiotta, jos näyttää siltä, että on hätätilanne.

Kysymys 13
Valitse seuraavista vaihtoehdoista kaikki oikeat.
Tietoturvallisuudesta huolehtiminen kuuluu osaksi jokaisen terveydenhuollon toimintayksikön tehtäviä, koska:

A) Tietojen luottamuksellisuuden säilyttämisestä on säädetty lailla.
B) Verkkohyökkäys tietojärjestelmiin voi estää näiden käyttöä terveydenhuollon apuna ja siten jopa vaarantaa potilaiden hoidon.
C) Oikeudettomat muutokset tietoihin tai tietojärjestelmiin voivat vaarantaa tietojen luotettavuuden siten, ettei tietoja voi enää lainkaan käyttää.
D) Sivullisten pääsy luottamuksellisiin tietoihin voi vaarantaa sekä potilaiden turvallisuuden että aiheuttaa rangaistuksia terveydenhuollon toimintayksikölle tai sen työntekijöille.

Kysymys 14
Valitse seuraavista kaikki oikeat vaihtoehdot.
Sinun täytyy vaihtaa salasanasi:

A) Kun epäilet, että salasanasi on paljastunut.
B) Kun järjestelmä käskee.
C) Kerran kuukaudessa, esimerkiksi kuukauden ensimmäisenä arkipäivänä.
D) Kun kollegasi pyytää sinua vaihtamaan salasanasi.

Kysymys 15
Valitse seuraavista kaikki oikeat vaihtoehdot.
Taataksesi, että muistat salasanasi vaivatta etkä hukkaa niitä, voit:

A) Kirjoittaa salasanasi paperille.
B) Säilyttää salasanojasi tiedostossa.
C) Säilyttää salasanojasi matkapuhelimesi muistissa.
D) Vaihtaa salasanasi lähimmän kollegasi kanssa.

Kysymys 16
Valitse seuraavista kaikki oikeat vaihtoehdot.
On hyvä:

A) Käyttää samaa salasanaa sekä työsähköpostissasi että kotisähköpostissasi, jotta salasanasi olisi helpompi muistaa.
B) Käyttää salasanaa, joka sivullisen on mahdotonta arvata.
C) Uudelleenkäyttää hyväksi havaittuja salasanoja, koska niiden kirjoittaminen on nopeaa, eikä sivullinen voi helposti nähdä, mitä näppäimistöllä kirjoitat.
D) Lähettää salasanasi tietohallintoyksikköön virheiden välttämiseksi.

Kysymys 17
Valitse seuraavista salasanoista kaikki, jotka edustavat hyvää esimerkkiä laadukkaasta salasanasta.

A) Keskussairaala123
B) Qwertyuiop.
C) Beaut1ful&Weather!_
D) NOSKCAJ_LEAHCIM

Kysymys 18
Valitse seuraavista vaihtoehdoista kaikki oikeat.
Voin edelleen lähettää kiertokirjeenä kulkevan sähköpostin, jos:

A) Siinä ei ole liitetiedostoja.
B) Se on peräisin luotettavasta lähteestä.
C) Sisältö liittyy terveydenhuollon palveluihin, tai kyseessä on keräys hyvän asian puolesta.
D) Kyseessä on varoitusviesti esimerkiksi liikkeellä olevasta viruksesta.

Kysymys 19
Valitse seuraavista väittämistä kaikki oikeat.

A) Jos sähköpostiviestin lähettäjä on ystäväni ja tiedän hänen käyttävän uusinta virustorjuntaa, voin avata häneltä sähköpostitse liitetiedostona tulleen suoritettavan ohjelman tarkastamatta sitä erikseen.
B) Jos sähköpostin otsikkorivi on epäilyttävä, en avaa sähköpostia yrittämättä ensin varmistaa sen oikeellisuutta esimerkiksi ottamalla yhteyttä lähettäjään.
C) Ladatessani tiedostoja Internetistä saan käyttää ainoastaan luotettuja ja maineikkaita sivustoja.
D) On hyvä ottaa tärkeistä tiedostoista oma varmuuskopio, tai säilyttää tiedostoja sellaisella verkkolevyllä, että varmuuskopio otetaan tietohallinnon toimesta automaattisesti.

Kysymys 20
Valitse seuraavista vaihtoehdoista kaikki oikeat.
Terveydenhuollon ammattihenkilö ei saa kertoa sivulliselle:

A) Yksikössään hoidossa olleen potilaan nimeä.
B) Yksikössään hoidossa olleen potilaan henkilötunnusta.
C) Yksikössään hoidossa olleen potilaan terveydentilaan liittyviä seikkoja.
D) Yksikössään hoidossa olleen potilaan perheestä ilmi tulleita asioita.

Kysymys 21
Valitse seuraavista vaihtoehdoista kaikki oikeat.
Jos henkilö työtehtäviä hoitaessaan tai muutoin rikkoo henkilötietojen käsittelystä säädettyjä lakeja tai salassapitovelvoitetta, seuraamuksena voi olla:

A) Sakkorangaistus.
B) Vankeusrangaistus.
C) Ammatinharjoittamisoikeuden rajoittaminen tai poistaminen.
D) Kirjallinen varoitus.

Kysymys 22
Valitse seuraavista vaihtoehdoista kaikki ne, jotka ovat esimerkkejä potilasasiakirjoista.

A) Lähetteet.
B) Laboratoriotutkimusten tulokset.
C) Lääkärintodistukset.
D) Ajanvaraustiedot.

Kysymys 23

Valitse seuraavista väittämistä kaikki oikeat.

A) Sähköpostin käyttöä valvotaan, sähköpostiviestejä tarkkaillaan ja tarvittaessa suodatetaan haittaohjelmilta suojautumiseksi.
B) Virustorjunta täytyy päivittää säännöllisesti.
C) Lähettäessäsi sähköpostiviestejä et saa liittää viesteihisi liitetiedostoja.
D) Sinun täytyy käyttää tietokoneessasi näytönsäästäjää (screen saver), jonka salasana on aktivoitu käyttöön.

Kysymys 24

Valitse seuraavista vaihtoehdoista kaikki oikeat.

Virukset voivat levitä tietokoneeseesi:

A) Sähköpostin välityksellä.
B) Internetissä olevilta verkkosivuilta.
C) CD-levyillä tai korpuilla olevista tiedostoista.
D) Sähköverkosta silloin, kun tietokoneesi verkkovirta on kytkettynä päälle.

Kysymys 25

Valitse seuraavista vaihtoehdoista kaikki oikeat.

Tietokoneesi voi olla viruksen saastuttama, jos:

A) Tiedostojesi sisältö on odottamattasi muuttunut.
B) Viruksentorjuntaohjelmisto näyttää varoitus- tai hälytysviestin.
C) Tietokoneesi toimii normaalia hitaammin.
D) Tietokoneesi uudelleenkäynnistyy itsekseen ilmoittamatta siitä minkäänlaisella varoitusviestillä.

Vastauslomake

Ensimmäinen kysymysosio

Kunkin seuraavan kysymyksen vastaukseksi sopii esitetyistä vaihtoehdoista täsmälleen yksi, joka on joko ainoa täysin oikea tai sellainen, joka parhaiten kuvaa lähinnä olevaa oikeaa vaihtoehtoa. Valitse siis kuhunkin kysymykseen neljästä vastausvaihtoehdosta yksi.

Jokaisesta annetusta oikeasta vastauksesta saat yhden pisteen ja väärästä nolla pistettä, vaikka keskustelu ja siinä saatu tulkinta osoittaisikin vastauksesi oikeaksi. Tämän osion maksimipistemäärä on 10.

Kysymys	Vastauksesi				Pistemääräsi
1	A ☐	B ☐	C ☐	D ☐	____
2	A ☐	B ☐	C ☐	D ☐	____
3	A ☐	B ☐	C ☐	D ☐	____
4	A ☐	B ☐	C ☐	D ☐	____
5	A ☐	B ☐	C ☐	D ☐	____
6	A ☐	B ☐	C ☐	D ☐	____
7	A ☐	B ☐	C ☐	D ☐	____
8	A ☐	B ☐	C ☐	D ☐	____
9	A ☐	B ☐	C ☐	D ☐	____
10	A ☐	B ☐	C ☐	D ☐	____
Yhteensä					**____ / 10**

Toinen kysymysosio

Kussakin seuraavassa kysymyksessä vastaukseksi sopii esitetyistä vaihtoehdoista mikä tahansa määrä vastauksia (0–4 oikeaa vastausta). Huomaa siis, että kaikki tietyn kysymyksen vaihtoehdot voivat olla vääriä tai vastaavasti myös oikeita. Valitse kuhunkin kysymykseen kaikki mielestäsi kelpaavat vaihtoehdot.

Saat annetusta oikeasta vastauksesta yhden pisteen ja väärästä nolla pistettä.

Kysymys	Vastauksesi				Pistemääräsi
11	A ☐	B ☐	C ☐	D ☐	____
12	A ☐	B ☐	C ☐	D ☐	____
13	A ☐	B ☐	C ☐	D ☐	____
14	A ☐	B ☐	C ☐	D ☐	____
15	A ☐	B ☐	C ☐	D ☐	____
16	A ☐	B ☐	C ☐	D ☐	____
17	A ☐	B ☐	C ☐	D ☐	____
18	A ☐	B ☐	C ☐	D ☐	____
19	A ☐	B ☐	C ☐	D ☐	____
20	A ☐	B ☐	C ☐	D ☐	____
21	A ☐	B ☐	C ☐	D ☐	____
22	A ☐	B ☐	C ☐	D ☐	____
23	A ☐	B ☐	C ☐	D ☐	____
24	A ☐	B ☐	C ☐	D ☐	____
25	A ☐	B ☐	C ☐	D ☐	____
Yhteensä					**____ / 15**

Yhteispisteet

Laske alla olevaan taulukkoon yhteispisteesi. Voit arvioida omaa osaamistasi taulukossa olevan neuvoa-antavan pisteytyksen avulla.

Osio	Pistemääräsi
1	**____ / 10**
2	**____ / 15**
Yhteensä	**____ / 25**

Pistemäärä
23–25 Erittäin hyvä
20–22 Hyvä
17–19 Tyydyttävä
14–16 Paremminkin voisi mennä
Alle 14 …

Kysymyslomakkeen vastaukset perusteluineen

Ohjeita

Seuraavassa on esitettynä kysymysten oikeat vastaukset ja vaihtoehdot perusteluineen. Huomaa, että moni kysymys tai vaihtoehto voi olla tulkinnanvarainen. Oikeaksi esitetty vastausvaihtoehto ei välttämättä ole ainoa oikea, vaan voi vaihdella tilanteen mukaan. Esimerkiksi:

- Kaikilla ei ole mahdollisuutta lukita työasemaa, koska työasemat ovat yhteiskäyttöisiä.
- Turvapolitiikka pakottaa käyttäjän valitsemaan tietynlaatuisen salasanan.
- Lainsäädännön osalta on esitetty kokooma voimassa olevaa lakitekstiä esimerkinomaisesti. Kunkin lain tulkinnan osalta on olemassa nykykäytäntö, johon koulutuksessa ei oteta eikä ole tarkoituskaan ottaa kantaa. Koulutusmateriaalin laatijan, kouluttajan tai koulutukseen osallistujan ei ole myöskään tarkoitus muodostaa koulutuksen perusteella omaa laintulkintaa.
- Lainsäädäntöön liittyen voi olla olemassa myös poikkeuksia (esimerkiksi alueellinen lainsäädäntö Kainuussa).

Kuhunkin kysymykseen esitetyt vaihtoehdot on kaikki syytä käydä läpi koulutuksen palauteosuudessa. Vaikka vaihtoehto (oikea/väärä) tuntuisi itsestäänselvyydeltä, on tärkeää mainita esimerkiksi seuraamukset, mitä väärästä toiminnasta voi olla.

Mukana on myös pisteytysohje muutamaan kohtaan. Tämäkin on kuitenkin vain keskustelun herättämiseksi. Kyseessähän ei ole testi, vaan harjoitus. Itsetarkoitus ei ole laskea pisteitä, vaan lisätä koulutukseen osallistujan tietoturvatietoisuutta.

HUOMAA, että tässä paperissa olevat oikeat vastaukset on tarkoitettu kouluttajan avuksi keskusteluosuutta varten. Tätä dokumenttia ei ole missään nimessä tarkoitus jakaa sellaisenaan koulutettaville. Vastaukset on ehdottomasti aina esitettävä koulutukseen osallistujalle tarpeellisine perusteluineen suullisesti, mielellään käymällä avointa keskustelua yhdessä koulutettavien kanssa. Tämä voi luoda huomattavan suuren riskin väärintulkinnoille ja väärinymmärryksille, mitä pitää ehdottomasti välttää. Materiaali on nimenomaan osa koulutusmateriaalia, osa ”tietoturvahengen” luomista, eikä siten edusta minkäänlaista tulkintaa lainsäädännöstä tai organisaatioissa voimassa olevista ohjeista.

Ensimmäinen kysymysosio

Kysymys 1
Mikä seuraavista vaihtoehdoista kuvaa parhaiten sitä tahoa, jolle voit kertoa havaitsemastasi tai epäilemästäsi tietoturvaongelmasta?

E) Sanomalehti, televisio tai muu media.
F) Poliisiviranomainen.
G) Organisaatiosi tietoturvallisuuspäällikkö.
H) Lähin kollegasi.

Esitetyistä vaihtoehdoista oikea on kohta C, josta yksi piste. Jos organisaatiossa ei ole nimettyä turvallisuuspäällikköä, sellainen on syytä nimetä pikimmiten.

Muista vaihtoehdoista D ei myöskään ole ehdottoman väärin: jos halutaan saivarrella ja tietoturvapäällikkö on nimenomaan henkilön oma esimies, voisi myös kohdan D hyväksyä oikeana. Tämä saattaa olla myös mahdollista, mikäli organisaatiossa ei vielä ole nimettyä tietoturvapäällikköä. Riippuen ongelman laadusta, joissakin tapauksissa kohta B voitaisiin hyväksyä: erityisesti silloin, kun tietoturvaongelma on osa jotakin muuta ongelmaa (esimerkiksi varkaita konesalitiloissa), poliisille tulisi samalla raportoitua myös tietoturvaloukkaus. Tärkeää on huomata, että mahdollinen ilmoitus poliisille ei tietenkään poista vaatimusta raportoida ongelmasta myös organisaation sisällä. Kohta A on selkeästi väärin, eikä sitä voi missään tapauksessa pitää oikeana.

Kysymys 2
Mikä seuraavista on vähimmäisvaatimus hyvälle salasanalle?

A) Kaikki salasanat ovat hyviä, eikä vähimmäisvaatimusta ole.
B) Vähintään viisi merkkiä pitkä.
C) Vähintään kymmenen merkkiä pitkä, joista yhden täytyy olla numero tai erikoismerkki.
D) Vähintään viisitoista merkkiä pitkä, joista vähintään yhden täytyy olla numero ja vähintään yhden erikoismerkki.

Esitetyistä vaihtoehdoista oikea on kohta C, josta yksi piste. On huomattava, että tämä vaatimus ei pelkästään ole riittävä: esimerkiksi keskussairaala1 ei kelpaa laadukkaaksi salasanaksi, mutta A7!bat9o9S kelpaa (kunhan käyttäjä itse muistaa sanan kirjaamatta sitä ylös).

Myös kohta D voidaan hyväksyä oikeana. Jos joku henkilökohtaisesti tulkitsee näin tiukan salasanavaatimuksen, tai jos tällainen salasanapolitiikka on jossakin käytössä, on tämä pelkästään positiivista. Tällöin täytyy tietysti muistaa muut salasanojen valintaan ja käyttöön kohdistuvat vaatimukset kuten edellä: ei saa kirjoittaa muistiin; ei saa olla liian yksinkertainen arvattavaksi tai sanakirjahyökkäyksen kohteeksi (esimerkiksi ”123POLIKLINIKKA.”). Kohdat A ja B eivät missään tapauksessa ole oikeita, vaikka järjestelmä ja sovellus näiden mukaisen salasanan hyväksyisivätkin.

Vaatimuksia hyvälle ja laadukkaalle salasanalle on riittävän pituuden lisäksi muitakin. Näistä mainittakoon esimerkiksi erikoismerkkien käyttö (silloin, kun se järjestelmän puolesta on mahdollista), vaikea arvattavuus (ei johdannainen käyttäjätunnuksesta, omasta nimestä tai muusta tutusta asiasta) ja originaalisuus (”ei löydettävissä sanakirjasta”, vaan mielellään jonkinlainen kombinaatio erilaisia sanoja ja merkkejä). Lisäksi salasanakäytäntöihin (ei luovuteta, ei kirjata paperille, vaihdetaan riittävän usein, kirjoitettaessa noudatetaan varovaisuutta ulkopuolisilta tarkkailijoilta) on olemassa erilaisia ohjeita. Nämä vaihtelevat kuitenkin organisaatioittain ja teknologioittain.

Kysymys 3

Seuraavista väittämistä ainoastaan yksi on oikea. Mikä?

E) Voit olla välittämättä copyright-merkinnästä ja tehdä ohjelmistosta kopion väliaikaiseen tai tilapäiseen käyttöön, jos se on työtehtäviesi hoidossa välttämätöntä.

F) Jos saat tietoosi administraattorin (järjestelmänhoitaja) salasanan, voit muuttaa oman käyttäjätunnuksesi asetuksia ja oikeuksia silloin, kun kyseessä on hätätilanne tai muutoin erittäin tärkeä asia, josta sinun täytyy huolehtia.

G) Kun palvelussuhteesi työnantajan kanssa on loppunut, voit mainita ystävillesi yksikössäsi hoidettavana olleen julkisuuden henkilön nimen, kunhan et mainitse mitään hänen terveydentilastaan.

H) Jos työtehtävissä käyttämäsi kannettavan tietokoneen kovalevy hajoaa, et voi irrottaa kovalevyä itse, viedä sitä huoltoon ja jättää korjattavaksi, vaikka välttämättä tarvitsisit konetta työtehtäviesi hoidossa ja huoltotarve olisi kiireellinen.

Esitetyistä vaihtoehdoista oikea on kohta D, josta yksi piste. Kovalevyllä saattaa olla arkaluonteista tietoa esimerkiksi välimuistitiedostoissa, vaikkeivät ohjelmistot tai tietokannat olisikaan kannettavassa tietokoneessa.

Kohta A on laiton. Luvaton kopiointi on aina rikos eikä sitä voi perustella tarpeella. Myös kohta B on laiton ja voidaan pahimmassa tapauksessa tulkita tietomurroksi. Kohta C on myös laiton: luottamuksellisuus ja salassapito koskevat myös työsuhteen loppumisen jälkeistä aikaa.

Kysymys 4

Seuraavista väittämistä ainoastaan yksi on oikea. Mikä?

E) Voit liittää kollegasi sähköpostiosoitteen ainoastaan sellaiselle postituslistalle, jossa käsitellään asioita, jotka auttavat kollegaasi hänen työtehtäviensä hoidossa.

F) Voit tallettaa sähköpostissa saamasi liitetiedoston oman tietokoneesi kovalevylle.

G) Suojellaksesi lähettämiesi viestien luottamuksellisuutta voit ottaa käyttöösi salausohjelmiston ja luoda oman avainparin, jonka avulla voit salata kaikki lähettämäsi viestit.

H) Voit vaihtaa henkilökohtaisen käyttäjätunnuksesi ja salasanasi lähimmän kollegasi kanssa hänen vastaavaan tunnukseensa ja salasanaansa, jos voitte näin toimia toistenne varahenkilöinä tai tästä vaihdosta on teille muuten apua työtehtävienne hoidossa.

Esitetyistä vaihtoehdoista oikea on kohta B, josta yksi piste. Huomaa, että jos organisaation tietoturvapolitiikka tämän kieltää, ei vaihtoehdoista yksikään ole oikea.

Vaihtoehto A on joka tapauksessa väärin. Muiden henkilöiden sähköpostiosoitteita ei koskaan pidä laittaa minkäänlaisille (muiden henkilöiden kuin itsesi ylläpitämille) jakelulistoille tai esimerkiksi uutiskirjeiden postituslistoille. Tietoja hyväksi havaituista jakelulistoista voi toki postittaa kollegoille, jolloin he itse voivat päättää osoitteensa liittämisestä. Vaihtoehto C:n mukainen avainten luonti ja varmenteen käyttöönotto voidaan joissakin organisaatioissa sallia, mutta teknisesti vaihtoehto on väärin. Omaa avainparia ei käytetä viestin salaamiseen vaan allekirjoitukseen. Salaus tehdään vastaanottajan avaimen (varmenteen) avulla. Vaihtoehto D ei ole suositeltava. Joissakin organisaatioissa joissakin sovelluksissa on yhteiskäyttöisiä tai jaettuja tunnuksia, tai kyseinen toiminta on politiikan sallimaa. Näin ei kuitenkaan ole syytä olla. Vaikkei tästä näyttäisi olevan haittaa, ja se tukisi organisaation toimintaa, se rikkoo työntekijöiden oikeusturvaa (mahdollisten vahinkojen yhteydessä oikean henkilön selvittäminen voi olla työlästä) eikä täten noudata tai toteuta lain edellyttämää hyvää tiedonhallintatapaa.

Kysymys 5

Seuraavista väittämistä ainoastaan yksi on oikea. Mikä?

E) Voit lähettää sähköpostilla liitetiedostoja välittämättä niiden koosta, koska vastaanottajan sähköpostijärjestelmä huolehtii liian suurien tai mahdollisesti muuten sopimattomien liitetiedostojen oikeanlaisesta käsittelystä.

F) Sähköpostiohjelmistoissa löytyy ominaisuus, jonka avulla voit lähettää sähköpostiviestin useille henkilöille yhtaikaa ilman, että vastaanottajat näkevät toistensa sähköpostiosoitteita.

G) Jos vastaanotat viruksesta varoittavan viestin esimerkiksi sähköpostitse, se kannattaa lähettää eteenpäin mahdollisimman monelle kollegallesi ja muille tuttavillesi.

H) Voit pitää tai tallettaa rajoittamattoman määrän vastaanottamiasi sähköpostiviestejä sähköpostipalvelimella välittämättä niiden mahdollisesti viemästä levytilasta, sillä sama levytila kuluu tallennettaessa viestit ja liitetiedostot esimerkiksi verkkolevylle.

Esitetyistä vaihtoehdoista oikea on kohta B, josta yksi piste (esimerkiksi Piilokopio-kenttä, Bcc-kenttä).

Kohta A on väärin: henkilön pitää kiinnittää huomiota tiedostokokoon lähettäessään erityisen suuria liitetiedostoja. Normaalikäytössä esimerkiksi muutaman megatavun liitetiedostot ovat vielä kohtuullisen tavallisia eivätkä yleensä aiheuta teknisiä tai muita ongelmia. Kohta C on väärin: virusvaroitus- ja muut vastaavat viestit lähetetään aina tietohallinnon tai tietoturvayksikön toimesta. Saadessaan virusvaroitusviestin (muualta kuin em. tahoilta) on yleensä syytä olla tekemättä mitään. Tietohallinto- ja tietoturvayksikkö saavat aiheelliset varoitusviestit myös muuta kautta ja luultavasti huomattavasti ennen kuin organisaation sisältä, ja heidän työnkuvaansa myös kuuluu seurata tietoturvatilannetta. Tästä syystä on turha kuormittaa varoitusviestillä heidän toimintaansa, ellei näe siihen erityistä syytä. Tärkeintä on käyttää normaalijärkeä tilanteen arvioinnissa. Jos on epävarma ja kokee varoitusviestin aiheelliseksi, on perusteltua lähettää se eteenpäin tietohallintoon tai tietoturvayksikköön. Vaihtoehto D on väärin: sähköpostijärjestelmää ei ole syytä käyttää viestien varastona tai arkistona. Verkkolevy (josta otetaan säännölliset varmistukset) on sopiva paikka viestiarkistolle.

Kysymys 6

Valitse seuraavista vaihtoehdoista mielestäsi paras. Jos epäilet, että haittaohjelma on saastuttanut tietokoneesi, mitä seuraavista vaihtoehdoista **ei** ole suositeltavaa tehdä?

E) Kytke tietokoneesi irti tietoverkosta.

F) Uudelleenkäynnistä tietokoneesi välittömästi.

G) Kirjaa ylös varoitus- tai muu viesti, joka mahdollisesti on näkynyt tietokoneesi näytöllä.

H) Ota yhteyttä tietohallintoon.

Esitetyistä vaihtoehdoista oikea on kohta B, josta yksi piste. Tietokonetta ei siis ole syytä uudelleenkäynnistää. Jos tietokone on jo saastunut, ei uudelleenkäynnistys auta mitään. Päinvastoin: jotkut haittaohjelmat saattavat saada käynnistyksessä uutta ”puhtia” ja saada aikaan muita haittavaikutuksia. Haittaohjelma saattaa esimerkiksi aktivoitua tekemään erilaisia tuhoamis- tai muutostoimia tietokoneen tiedostoihin tai määrityksiin, jonka jälkeen torjuntatyö saattaa olla jopa mahdotonta.

Jos epäilee tietokoneensa olevan haittaohjelman saastuttama, on syytä kytkeä kone irti tietoverkosta estääkseen mahdollisen tartunnan leviämisen. Jotta tilanteen selvitys olisi mahdollisimman tehokasta, kaikki virheilmoitukset on syytä kirjata ylös mahdollisuuksien mukaan. Yhteydenotto tietohallintoon tai tietoturvayksikköön aloittaa mahdollisen ongelman selvittämisen.

Kysymys 7

Seuraavista vaihtoehdoista ainoastaan yksi on oikea. Mikä?

Kuka seuraavista vastaa siitä, että toimintayksiköissä on saatavilla kirjalliset ohjeet potilasasiakirjoihin sisältyvien tietojen käsittelystä ja menettelytavoista?

E) Toimintayksikön terveydenhuollosta vastaava johtaja.
F) Toimintayksikön tietohallintopäällikkö.
G) Toimintayksikköön nimetty tietoturvallisuuspäällikkö.
H) Kulloinkin vastuussa oleva johtava ylilääkäri.

Esitetyistä vaihtoehdoista oikea on kohta A, josta yksi piste. Sosiaali- ja terveysministeriön asetuksessa potilasasiakirjojen laatimisesta ja säilyttämisestä todetaan toimintayksikön johtajan toimivan rekisterinpitäjän edustajana. Tätä vastuuta toimintayksikön johtaja ei voi sopimuksellisesti tai itse toisin määräämällä siirtää organisaatiossaan toisaalle.

Edellä mainitun perusteella kohdat B, C ja D ovat väärin eikä lisäperusteluja kaivattane. Käytännön ohjeistuksen laatimisen ja jakelun toimintayksikön johtaja on toki luultavasti vastuuttanut organisaatiossaan sopivalle taholle, mutta lakisääteinen vastuu ei tällä toimenpiteellä siirry. Toki D voi olla oikein siinä tapauksessa, että terveydenhuollosta vastaava johtaja toimii johtavana ylilääkärinä.

Kysymys 8

Seuraavista väittämistä ainoastaan yksi on oikea. Mikä?

E) Hävittäessäsi luottamuksellista materiaalia voit laittaa sen mihin tahansa roskalaatikkoon toimintayksikön alueella.
F) Jos sinulla on vieraita työpaikallasi, voit kuljettaa heitä välittämättä vierailijoiden kirjaussäännöstä, mikäli teillä on kiire, ja turha kirjausprosessi hidastaisi toimintaanne kohtuuttomasti.
G) Sinun ei tarvitse erikseen huolehtia työpöydälläsi tai näyttöpäätteelläsi näkyvistä arkaluonteisista tai luottamuksellisista tiedoista, sillä kenelläkään ei ole mitään asiaa huoneeseesi.
H) Potilasasiakirjoihin sisältyviä tietoja voidaan luovuttaa sivulliselle ainoastaan potilaan kirjallisella suostumuksella.

Esitetyistä vaihtoehdoista oikea on kohta D, josta yksi piste. On huomattava, että tietyissä erityistilanteissa ja tietyille sivullisille tahoille (kuten Kela, poliisiviranomainen, kunnallinen sosiaaliviranomainen) tietoja luovutettaessa ei välttämättä tarvita potilaan kirjallista lupaa. Nämä tilanteet ilmenevät laissa potilaan asemasta ja oikeuksista.

Kohta A on väärin, mutta jos organisaatiossa ei ole varattu luottamuksellista ja arkaluonteista materiaalia varten asianmukaista tuhoamismenettelyä (silppurit, tietoturvaroskikset ym.), tämä voi aiheuttaa vääriä vastauksia. Kohta B on selkeästi väärin riippumatta mahdollisesta kiireestä tai muista olosuhteista. Jos kyseessä on hätätilanne, esimerkiksi evakuointi, ei esimerkiksi uloskirjausta tietenkään tarvita, jos se voi vaarantaa ihmisten terveyden tai fyysisen turvallisuuden. Kohta C on yksiselitteisesti väärin: luottamuksellista tietoa on käsiteltävä asianmukaista huolellisuutta ja salassapitosäännöksiä noudattaen. Näyttöpäätteelle jättäminen ei noudata hyvää tiedonhallintatapaa missään tiloissa.

Kysymys 9
Seuraavista vaihtoehdoista ainoastaan yksi on oikea. Mikä?
Potilasasiakirjojen, näytteiden ja mallien säilytys sosiaali- ja terveysministeriön asetuksella säädetyn säilytysajan päätyttyä:

E) On ehdottomasti kiellettyä, ja ne on aina hävitettävä asetuksen mukaisesti.
F) On mahdollista Arkistolaitoksen luvalla.
G) On mahdollista toimintayksikön tietohallintopäällikön luvalla.
H) On mahdollista, jos se on välttämätöntä potilaan hoidon takia.

Esitetyistä vaihtoehdoista oikea on potilaan asemasta ja oikeuksista säädetyn lain perusteella (12 §) kohta D, josta yksi piste.

Kohta D kumoaa yksiselitteisesti kohdan A, joka on siis väärin. Kohta B on väärin, mutta se voi periaatteessa sisältää poikkeuksia edellä mainittuun Arkistolain perusteella (esimerkiksi 18. ja 28. päivä syntyneet). Kyseessä ei kuitenkaan ole Arkistolaitoksen lupa. Kohta C on väärin, eikä tietohallintopäällikkö luultavasti ole se taho, joka toteuttaisi laissa mainittua arviointivelvollisuutta (jos halutaan saivarrella sillä, että periaatteessa arvioinnin suorittaja antaa säilytykseen luvan).

Kysymys 10
Seuraavista vaihtoehdoista ainoastaan yksi on oikea. Mikä?
Terveydenhuollon ammattihenkilön sanelun perusteella tehtyjen merkintöjen oikeellisuudesta vastaa:

E) Sanelija.
F) Merkintöjen tekijä.
G) Tietohallintoyksikkö, jos se on antanut käyttöön välineet merkintöjen tekemiseksi sanelun perusteella.
H) Kulloinkin vastuussa oleva johtava ylilääkäri.

Esitetyistä vaihtoehdoista oikea on potilasasiakirjojen laadinnasta annetun asetuksen perusteella kohta A, josta yksi piste.

Laki on asiassa yksiselitteinen, joten kohdat B, C ja D ovat väärin. Kuitenkin on huomattava, että oikeustapauksia ja siten lain tulkintaa ei joko ole tai oikeustapauksia on erittäin rajallinen määrä.

Toinen kysymysosio

Kysymys 11
Valitse seuraavista kaikki oikeat vaihtoehdot.
Kuka on vastuussa tietoturvan toteutumisesta toimintayksikössäsi?

E) Toimintayksikön johtaja.
F) Kaikki esimiesasemassa olevat.
G) Tietohallintoyksikkö.
H) Jokainen työntekijä.

Esitetyistä vaihtoehdoista kaikki ovat oikeita. Jos vaihtoehto D on valittu, yksi piste. Muussa tapauksessa nolla pistettä.

Kysymys 12
Valitse seuraavista tietoturvapolitiikkaa koskevista väitteistä kaikki oikeat.

E) Tietoturvapolitiikka on tietohallintoyksikön käyttöön tarkoitettu ohje, joka sisältää hyviä ajatuksia tietoturvallisuuden kehittämisestä ja jonka avulla ylläpidetään tietoturvallisuutta terveydenhuollon eri toimintayksiköissä.
F) Tietoturvapolitiikka sisältää päivittäisiä tietoturvaohjeita järjestelmien vastuuhenkilöille.
G) Tietoturvapolitiikka on toimintayksikön johdon hyväksymä ja koko toimintayksikön laajuisesti käyttöön määräämä.
H) Voit jättää tietoturvapolitiikan huomiotta, jos näyttää siltä, että on hätätilanne.

Esitetyistä vaihtoehdoista kohta C on oikein. Tästä yksi piste.

Huomaa, että kaikki seuraavat vaihtoehdot voivat aiheuttaa saivartelua. Kohta A: tietoturvapolitiikka on koko organisaation, ei ainoastaan tietohallintoyksikön käyttöön tarkoitettu. Kohta B: politiikka ei sisällä päivittäisiä ohjeita vastuuhenkilöille. Kohta D on tulkittavissa tietyissä tilanteissa oikeaksi: jos kyseessä on esimerkiksi evakuointi tai potilaan hengen tai terveyden vaarantuminen, ei tietoturvapolitiikan ohjeita luonnollisesti välttämättä voi noudattaa. Tässä(kin) yhteydessä on välttämätöntä käyttää tervettä järkeä ja harkintaa. Ei kuitenkaan voi olla itseisarvona, että jos NÄYTTÄÄ siltä, että on hätätilanne, politiikan voi oletuksena jättää noudattamatta.

Kysymys 13
Valitse seuraavista vaihtoehdoista kaikki oikeat.
Tietoturvallisuudesta huolehtiminen kuuluu osaksi jokaisen terveydenhuollon toimintayksikön tehtäviä, koska:

E) Tietojen luottamuksellisuuden säilyttämisestä on säädetty lailla.
F) Verkkohyökkäys tietojärjestelmiin voi estää näiden käyttöä terveydenhuollon apuna ja siten jopa vaarantaa potilaiden hoidon.
G) Oikeudettomat muutokset tietoihin tai tietojärjestelmiin voivat vaarantaa tietojen luotettavuuden siten, ettei tietoja voi enää lainkaan käyttää.
H) Sivullisten pääsy luottamuksellisiin tietoihin voi vaarantaa sekä potilaiden turvallisuuden että aiheuttaa rangaistuksia terveydenhuollon toimintayksikölle tai sen työntekijöille.

Esitetyistä vaihtoehdoista kaikki kohdat ovat oikein. Vain, jos kaikki on valittu, yksi piste. Jos halutaan, näistä voidaan käydä läpi esimerkkitapauksia. Myös koulutukseen osallistujilta kannattaa kysyä esimerkkejä.

Kysymys 14
Valitse seuraavista kaikki oikeat vaihtoehdot.
Sinun täytyy vaihtaa salasanasi:

E) Kun epäilet, että salasanasi on paljastunut.
F) Kun järjestelmä käskee.
G) Kerran kuukaudessa, esimerkiksi kuukauden ensimmäisenä arkipäivänä.
H) Kun kollegasi pyytää sinua vaihtamaan salasanasi.

Esitetyistä vaihtoehdoista kohdat A ja B ovat oikein. Huomaa kysymyksenasettelu: TÄYTYY. Jos A on valittu, annetaan yksi piste, muussa tapauksessa nolla pistettä.

Joissakin organisaatioissa tietoturva- tai salasanapolitiikka voi suositella kohtaa C. Näin ei kuitenkaan pitäisi olla: säännöllisin väliajoin tapahtuva salasanan vaihto luo uhkan, joskin erittäin pienen sellaisen, salasanan vakoilulle. Myös kohta D on tulkinnanvarainen: jos joku (kuka tahansa) pyytää sinua vaihtamaan salasanaa, on tapahtumaan sinänsä suhtauduttava kuin kohdassa A. Toisen henkilön pyytämä vaihto pitäisi kuitenkin arvioida normaalia järkeä käyttämällä, ja tarvittaessa ottaen yhteyttä tietohallintoon tai tietoturvayksikköön.

Kysymys 15
Valitse seuraavista kaikki oikeat vaihtoehdot.
Taataksesi, että muistat salasanasi vaivatta etkä hukkaa niitä, voit:

E) Kirjoittaa salasanasi paperille.
F) Säilyttää salasanojasi tiedostossa.
G) Säilyttää salasanojasi matkapuhelimesi muistissa.
H) Vaihtaa salasanasi lähimmän kollegasi kanssa.

Esitetyistä vaihtoehdoista kaikki ovat väärin. Vain tässä tapauksessa yksi piste, muutoin nolla.

Nämä ovat kuitenkin sääntöjä, joita vastaan usein rikotaan. On ensiarvoisen tärkeää saada tietojärjestelmien käyttäjät havaitsemaan uhkat. Jos ulkopuolinen pääsee heidän tunnuksillaan tietojärjestelmään, myös henkilön oma oikeusturva on kyseessä. On muistettava, että henkilön käyttäjätunnus ja salasana == henkilö itse. Henkilö vastaa siitä, että salasana on sellainen, että vain hän itse sen tietää ja muilla ei sitä ole mahdollisuutta selvittää. Kohta B voi tuottaa hiuksen halkomista. Tietojärjestelmissähän salasanoja säilytetään nimenomaan järjestelmän sisäisessä tiedostossa, tosin kryptatussa muodossa.

Kysymys 16
Valitse seuraavista kaikki oikeat vaihtoehdot.
On hyvä:

E) Käyttää samaa salasanaa sekä työsähköpostissasi että kotisähköpostissasi, jotta salasanasi olisi helpompi muistaa.
F) Käyttää salasanaa, joka sivullisen on mahdotonta arvata.
G) Uudelleenkäyttää hyväksi havaittuja salasanoja, koska niiden kirjoittaminen on nopeaa, eikä sivullinen voi helposti nähdä, mitä näppäimistöllä kirjoitat.
H) Lähettää salasanasi tietohallintoyksikköön virheiden välttämiseksi.

Esitetyistä vaihtoehdoista vain kohta B on oikein. Tästä yksi piste.

Kohdan A mukainen saman salasanan käyttö on ehdottomasti kiellettyä, myös helpon muunnoksen (esimerkiksi vain viimeinen numero eroaa). Kohta D on myös ehdottomasti väärin. Salasanoja ei pidä lähettää missään tapauksessa selkokielisenä millään medialla, eikä kirjoittaa muutenkaan ylös. Kohta C voi olla tulkinnanvaraisesti oikein, mutta tämä ei ole lähtökohta. Hyvät salasanat muunneltuina ja riittävän suurella kierrolla voivat olla suositeltavia, sillä tämä edesauttaa muistamista ja toisaalta vähentää muistiin kirjoittamisen tarvetta. Salasanakysymysten edessä ollaan usein dilemman edessä: on valittava kahdesta huonosta vaihtoehdosta vähemmän huono. Tuo vähemmän huono jää siis tulkinnan varaan. Tässäkin yhteydessä maalaisjärki on käyttökelpoinen apuväline.

Kysymys 17
Valitse seuraavista salasanoista kaikki, jotka edustavat hyvää esimerkkiä laadukkaasta salasanasta.

E) Keskussairaala123
F) Qwertyuiop.
G) Beaut1ful&Weather!_
H) NOSKCAJ_LEAHCIM

Esitetyistä vaihtoehdoista vain kohta C on oikein, josta yksi piste. Tähän voi tosin vaikuttaa voimassa oleva salasanapolitiikka ja ohjeistus. Kyseinen salasana on riittävän pitkä ja siinä on riittävä valikoima erikoismerkkejä, numeroita ja kirjaimia eri kirjasintyypillä. Lisäksi sana on kohtuullisen helppo muistaa, koska pohjana on kuitenkin selvästi ymmärrettävä ja muistettava ilmaus. Voi toki olla, että tämäkään ei joillekin henkilöille riitä, vaan halutaan käyttää vielä mo-

nimutkaisempia sanoja. Tämä on tietysti hyväksyttävää ja myös ”kaikki väärin” pitää hyväksyä neljän pisteen arvoiseksi.

Yleissääntönä kuitenkin A on liian helppo sanakirjahyökkäykselle (vain ensimmäinen kirjain isolla, toimialakohtainen sana, numerona 123 eikä esimerkiksi 394). B on suoraan näppäimistöltä (muutkaan ilmiselvät näppäimistösanat eivät ole suositeltavia, esimerkiksi zxcvASDFqwer1234). Kohdassa D huomio kiinnittyy sekä väärinpäin kirjoitukseen (MICHAEL_JACKSON) että siihen, että kaikki kirjaimet ovat samalla kirjasintyypillä ja että sanaan on sisällytetty vain yksi erikoismerkki.

Kysymys 18

Valitse seuraavista vaihtoehdoista kaikki oikeat.

Voin edelleen lähettää kiertokirjeenä kulkevan sähköpostin, jos:

E) Siinä ei ole liitetiedostoja.
F) Se on peräisin luotettavasta lähteestä.
G) Sisältö liittyy terveydenhuollon palveluihin, tai kyseessä on keräys hyvän asian puolesta.
H) Kyseessä on varoitusviesti esimerkiksi liikkeellä olevasta viruksesta.

Esitetyistä vaihtoehdoista kaikki ovat väärin. Vain tässä tapauksessa yksi piste, muutoin nolla.

Kiertokirjeitä ei ole syytä lähettää eteenpäin missään tapauksessa. Yksikään organisaatio ei varmasti suorita sisäistä tai ulkoista tiedonvälitystään kiertokirjetyyppisesti (poisluettuna esimerkiksi sisäinen lehtikierto), ja erityisesti sähköpostitse saamiinsa kiertokirjeisiin tulee aina suhtautua negatiivisesti. Oikeat varoitusviestit (esimerkiksi virusvaroitukset) tulevat aina suoraan siltä organisaatiolta, joka toiminnasta vastaa, ei koskaan kiertokirjeenä. Lisäksi kirjeen mukana voi kulkea viruksia, suuria liitetiedostoja, linkkejä arveluttaville sivustoille, tai yrityksiä saada haltuunsa organisaatioon liittyvää tietoa.

Kysymys 19

Valitse seuraavista väittämistä kaikki oikeat.

E) Jos sähköpostiviestin lähettäjä on ystäväni ja tiedän hänen käyttävän uusinta virustorjuntaa, voin avata häneltä sähköpostitse liitetiedostona tulleen suoritettavan ohjelman tarkastamatta sitä erikseen.
F) Jos sähköpostin otsikkorivi on epäilyttävä, en avaa sähköpostia yrittämättä ensin varmistaa sen oikeellisuutta esimerkiksi ottamalla yhteyttä lähettäjään.
G) Ladatessani tiedostoja Internetistä saan käyttää ainoastaan luotettuja ja maineikkaita sivustoja.
H) On hyvä ottaa tärkeistä tiedostoista oma varmuuskopio, tai säilyttää tiedostoja sellaisella verkkolevyllä, että varmuuskopio otetaan tietohallinnon toimesta automaattisesti.

Esitetyistä vaihtoehdoista kohdat B, C ja D ovat oikein. Jos B on valittu, annetaan yksi piste. Muutoin nolla.

Kohta A on joka tapauksessa väärin: liitetiedostojen osalta virustorjunta täytyy aina suorittaa riippumatta siitä, kuka on lähettäjä tai missä asemassa hän toimii. Joissakin organisaatioissa kohdan C mukainen tiedostojen lataus saattaa olla kielletty, jolloin myös tämä on väärin. Kohta B on tulkinnanvarainen: sähköpostitse yhteyden ottaminen (esimerkiksi vastaaminen outoon viestiin) ei ole suositeltavaa, koska alkuperäinen viesti saattaa esimerkiksi vain kalastaa toimivia sähköpostiosoitteita. Tässäkin kannattaa käyttää tervettä järkeä. Oletuksena kuitenkin kysymyksen tarkoituksena on kysyä oudosta otsikkorivistä, ei niinkään yhteydenotosta lähettäjään. Hyvä kuitenkin, jos tämä herättää keskustelua.

Kysymys 20

Valitse seuraavista vaihtoehdoista kaikki oikeat.
Terveydenhuollon ammattihenkilö ei saa kertoa sivulliselle:

E) Yksikössään hoidossa olleen potilaan nimeä.
F) Yksikössään hoidossa olleen potilaan henkilötunnusta.
G) Yksikössään hoidossa olleen potilaan terveydentilaan liittyviä seikkoja.
H) Yksikössään hoidossa olleen potilaan perheestä ilmi tulleita asioita.

Tässä kysymyksessä kaikki vastausvaihtoehdot ovat kiistatta oikeita (laki potilaan asemasta ja oikeuksista, henkilötietolaki), ja yksi piste annetaan ainoastaan silloin, kun kaikki vaihtoehdot on valittu. Kuten aiemmissakin kysymyksissä, myös tämän kysymyksen osalta on tiettyjä poikkeustapauksia, mutta niiden selvitys ei ole tämän kysymyksen tarkoitus.

Kysymys 21

Valitse seuraavista vaihtoehdoista kaikki oikeat.
Jos henkilö työtehtäviä hoitaessaan tai muutoin rikkoo henkilötietojen käsittelystä säädettyjä lakeja tai salassapitovelvoitetta, seuraamuksena voi olla:

E) Sakkorangaistus.
F) Vankeusrangaistus.
G) Ammatinharjoittamisoikeuden rajoittaminen tai poistaminen.
H) Kirjallinen varoitus.

Tässä kysymyksessä kaikki vastausvaihtoehdot ovat oikeita (rikoslaki ja useat erityislait), ja yksi piste annetaan ainoastaan silloin, kun kaikki vaihtoehdot on valittu. Saattaa olla, että oikeustapauksia ei ole, mutta kaikki vaihtoehdot ovat lain mukaan mahdollisia rangaistuksia. On lisäksi huomattava, että myös työnantaja voi määrätä (näistä poiketen ja näihin lisäten) myös muita seuraamuksia erilaisista työtehtävien suorittamisesta annettujen ohjeiden noudattamatta jättämisestä, luonnollisesti myös muista kuin salassapitovelvoitteiden rikkomisesta.

Kysymys 22

Valitse seuraavista vaihtoehdoista kaikki ne, jotka ovat esimerkkejä potilasasiakirjoista.

E) Lähetteet.
F) Laboratoriotutkimusten tulokset.
G) Lääkärintodistukset.
H) Ajanvaraustiedot.

Tässä kysymyksessä kaikki vastausvaihtoehdot ovat kiistatta oikeita, ja yksi piste annetaan ainoastaan siinä tapauksessa, että kaikki vaihtoehdot on valittu. Usein (tai aina) ajanvarausjärjestelmä on irrallinen potilastietojärjestelmästä eikä ajanvaraustietoja säilytetä potilastietojärjestelmässä. Tästä huolimatta ajanvaraustiedot liittyvät nimenomaan hoidon järjestämiseen ja ovat siten potilasasiakirjoja siinä missä röntgenkuvatkin (asetus potilasasiakirjojen laatimisesta). Ajanvaraustietojen säilyttämisajoista on säädetty potilasasetuksessa (muu potilasasiakirja-aineisto).

Kysymys 23

Valitse seuraavista väittämistä kaikki oikeat.

E) Sähköpostin käyttöä valvotaan, sähköpostiviestejä tarkkaillaan ja tarvittaessa suodatetaan haittaohjelmilta suojautumiseksi.
F) Virustorjunta täytyy päivittää säännöllisesti.
G) Lähettäessäsi sähköpostiviestejä et saa liittää viesteihisi liitetiedostoja.
H) Sinun täytyy käyttää tietokoneessasi näytönsäästäjää (screen saver), jonka salasana on aktivoitu käyttöön.

Esitetyistä vaihtoehdoista kohdat A, B ja D ovat oikein. Jos A on valittu, annetaan yksi piste, muutoin nolla pistettä.

Kohta C voi joissakin organisaatioissa olla kielletty, jolloin tämäkin täytyy hyväksyä oikeaksi vastaukseksi. Yleensä kuitenkin sähköpostiviestien liitetiedostot ovat sallittuja (esimerkiksi PDF-tiedostot). On huomattava, että kohtaa A säätelee laki yksityisyyden suojasta työelämässä sekä sähköisen viestinnän tietosuojalaki. On tarkoin määritelty, miten työnantaja voi valvontaa, seurantaa ja tarkkailua suorittaa. Kohdan D osalta voi olla tapauksia, että organisaatiossa on käytössä esimerkiksi jaetut työasemat tai käyttäjätunnukset (esimerkiksi usealla hoitajalla oma käyttöliittymä potilastietojärjestelmään samalla työasemalla), jolloin automaattista näytönsäästäjää tai edes näytön lukitusta ei voida käyttää. Vaikka tämä rikkoo työntekijän oikeusturvaa, kyseessä on nykyään pikemminkin käytäntö kuin poikkeus. Jos näin on, olisi ainakin sovellustasolla oltava mahdollisuus lukita oma sovellusikkunansa. Edellisen lisäksi kaikki osallistujat eivät välttämättä tiedä, mikä on näytönsäästäjä. Koulutuksen tarkoitus ei kuitenkaan ole tietotekniikan opetus, ja joitakin oletuksia voidaan tehdä. Tässä tapauksessa oletetaan, että jokainen osallistuja tietää, mikä on näytönsäästäjä.

Kysymys 24
Valitse seuraavista vaihtoehdoista kaikki oikeat.
Virukset voivat levitä tietokoneeseesi:

E) Sähköpostin välityksellä.
F) Internetissä olevilta verkkosivuilta.
G) CD-levyillä tai korpuilla olevista tiedostoista.
H) Sähköverkosta silloin, kun tietokoneesi verkkovirta on kytkettynä päälle.

Esitetyistä vaihtoehdoista kohdat A, B ja C ovat oikein. Vain, jos kaikki nämä on valittu (tai myös D on valittu näiden lisäksi), annetaan yksi piste. Muutoin nolla pistettä.

Kuitenkin, nykyteknologia mahdollistaa datasiirron sähköverkossa, ja tällaisen tiedonsiirron ollessa käytössä tietysti myös haittaohjelmat voivat sitä kautta levitä.

Kysymys 25
Valitse seuraavista vaihtoehdoista kaikki oikeat.
Tietokoneesi voi olla viruksen saastuttama, jos:

E) Tiedostojesi sisältö on odottamattasi muuttunut.
F) Viruksentorjuntaohjelmisto näyttää varoitus- tai hälytysviestin.
G) Tietokoneesi toimii normaalia hitaammin.
H) Tietokoneesi uudelleenkäynnistyy itsekseen ilmoittamatta siitä minkäänlaisella varoitusviestillä.

Esitetyistä vaihtoehdoista kaikki kohdat ovat oikein. Yksi piste annetaan ainoastaan, kun kaikki vaihtoehdot on valittu.

Tämä ei kaivanne selityksiä.

TYÖPAPEREITA-sarjassa aiemmin ilmestyneet

2007

Marita Päivärinne: Terveysvaikutusten arviointi Salossa. Uuden menetelmän omaksuminen päätöksentekoon
Työpapereita 10/2007 Tilausnro T10/2007

Tuija Portell & Maili Malin: Taustaa varhaiskasvatuksen laatukatsaukselle
Työpapereita 9/2007 Tilausnro T9/2007

Tarja Itkonen, Kaija Lindman, Harriet Corin, Anja Noro (toim.): Kokemuksia vanhustenhuollon vertailukehittämisestä ja RAI-tietojärjestelmästä
Työpapereita 8/2007 Tilausnro T8/2007

Minna Harjajärvi, Irma Kiikkala, Sami Pirkola: Puolitoista vuotta tsunamin jälkeen. Aasian luonnonkatastrofin seuraamusten psykososiaalinen hoito Suomessa
Työpapereita 7/2007 Tilausnro T7/2007

Matti Ojala, Ilkka Saario: Läketieteellisen hoidon haittavaikutusten kirjaamiskäytännön ja tilastoinnin kehittämisen asiantuntijaryhmän raportti
Työpapereita 6/2007 Tilausnro T6/2007

Kaija Lindman, Harriet Finne-Soveri, Sinikka Salo, Mauno Konttinen, Päivi Voutilainen ja Anja Noro: Vertailemalla yhteistyötä. Matkakertomus ja pilottitutkimus Sendaista
Työpapereita 5/2007 Tilausnro T5/2007

Mieli 2007. Kansallisten mielenterveyspäivien taustamateriaali, luennot ja posterit
Työpapereita 4/2007 Tilausnro T4/2007

Matti Mäkelä, Unto Häkkinen, Bengt Juslin, Päivi Koivuranta-Vaara, Antti Liski, Matti Lyytikäinen, Juha Laine: Sairaalasta kotiin asti. Erikoissairaanhoidosta alkaneet hoitojaksoketjut pääkaupunkiseudun kunnissa
Työpapereita 3/2007 Tilausnro T3/2007

Jan Klavus (toim.): Terveystaloustiede 2007
Työpapereita 2/2007 Tilausnro T2/2007

Maija Ritamo (toim.): X Terve Kunta -päivät. 23.–24.1.2007, Paasitorni, Helsinki
Työpapereita 1/2007 Tilausnro T1/2007

2006

Lauri Vuorenkoski, Mauno Konttinen, Minna Sinkkonen (toim.): Signaaleja. Stakesin tulevaisuusraportti 2007
Työpapereita 30/2006 Tilausnro T30/2006

Esa Eriksson, Tom Erik Arnkil, Marie Rautava: Ennakointidialogeja huolten vyöhykkeillä. Verkostokonsultin käsikirja – ohjeita verkostomaiseen työskentelyyn
Työpapereita 29/2006 Tilausnro T29/2006

Stakes ja Lääkehoidon kehittämiskeskus ROHTO: Potilas- ja lääkehoidon turvallisuussanasto
Työpapereita 28/2006 Tilausnro T28/2006

Tuomas Tenkanen: Ennakointidialogien käyttö päihdestrategiatyössä
Työpapereita 27/2006 Tilausnro T27/2006