Terveys- ja hyvinvointialojen opintokokonaisuus

Kyberturvallisuuskoulutuksen ja siihen liittyvän yhteistyön kehittäminen korkeakouluissa

© 2025 Ovaska Joonatan – Creative Commons 4.0 (CC BY-SA)

OPETUS- JA KULTTUURIMINISTERIÖ
UNDERVISNINGS- OCH KULTURMINISTERIET

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

05A – Pääsynhallinta

© 2025 Ovaska Joonatan – Creative Commons 4.0 (CC BY-SA)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Kulun- ja pääsynhallinta

Termistö

- Kulunvalvonta (Access Control)
  - Prosessi, jossa myönnetään tai evätään tietyt pyynnöt:
    - 1) hankkia ja käyttää tietoja ja niihin liittyviä tietojenkäsittelypalveluja
    - 2) päästä tiettyihin fyysisiin tiloihin (esim. henkilökunnantiloihin, sotilaslaitoksiin, salapidettävän tiedon tiloihin).
- Pääsynhallinta (Access Management / Access Control Management)
  - Käyttöoikeuksien hallinta on joukko käytäntöjä, jotka sallivat vain niille, joilla on lupa, suorittaa toiminnon tietylle resurssille. Kolme yleisintä pääsynhallintapalvelua, joita kohtaat päivittäin ehkä huomaamattasi, ovat:
    - Käytäntöjen hallinta, todennus ja valtuutus.
- Pääsynhallinta on laajempi kokonaisuus joka pitää sisällänsä kulunvalvonnan

jamk

Pääsynhallinta

Pääsynhallinnan ydinosa-alueet

- **Tavoite:** Pääsynhallinnan tarkoitus on estää hakkereita ja samalla sallia valtuutettujen käyttäjien tehdä kaikki tarvittava, mutta ei enempää kuin heille on sallittu.
- **Käyttäjätietokanta:** Tyypillisessä pääsynhallintajärjestelmässä on käyttäjätietokanta tai -hakemisto.
  - Tämä tietokanta sisältää tiedot siitä, kuka kukin käyttäjä on ja mitä he voivat tehdä tietojärjestelmässä.
  - Kun käyttäjät liikkuvat järjestelmässä, pääsynhallinta käyttää tietokannan tietoja heidän henkilöllisyytensä varmistamiseen, heidän toimintojensa seuraamiseen ja sen varmistamiseen, että he tekevät vain sen, mitä tietokanta sallii.

Lähde: https://www.ibm.com/topics/identity-access-management, viitattu 12.11.2024

jamk

Pääsynhallinta

Pääsynhallinnan ydinosa-alueet

- **Identiteetin elinkaaren hallinta**: Prosessi, jossa luodaan ja ylläpidetään käyttäjäidentiteettejä.
  - Käyttäjien luominen, päivittäminen ja poistaminen.
- **Pääsynvalvonta**: Käyttäjän oikeudet perustuvat työtehtävään ja vastuutasoon.
  - Käyttäjillä on vain vähimmäisoikeudet tehtävän suorittamiseen.
- **Autentikointi ja valtuutus**: Varmistaa käyttäjän henkilöllisyyden (esim. salasana, monivaiheinen tunnistautuminen (MFA)).
  - Määrittää, mihin resursseihin käyttäjä pääsee autentikoinnin jälkeen.
- **Identiteetin hallinta ja valvonta**: Käyttäjien toiminnan valvonta ja auditointijäljet.
  - Varmistaa, että yrityksen politiikat toimivat tarkoitetulla tavalla.

Lähde: https://www.ibm.com/topics/identity-access-management, viitattu 12.11.2024

jamk

Pääsynhallinta

Esimerkki – Sairaanhoitajan pääsyoikeudet

1. **Identiteetin elinkaaren hallinta**
   - Sairaanhoitajalle luodaan digitaalinen identiteetti, joka sisältää hänen nimensä, kirjautumistiedot, työnimikkeen ja käyttöoikeudet.
   - Tämä identiteetti tallennetaan sairaalan pääsynhallintajärjestelmän keskitettyyn tietokantaan.
2. **Pääsynvalvonta**
   - Sairaanhoitajan käyttöoikeudet perustuvat hänen rooliinsa ja vastuutasoonsa.
   - Esimerkiksi sairaanhoitaja voi:
     - Tarkastella potilastietoja ja kirjata hoitotoimenpiteitä.
     - Päästä käsiksi lääkkeiden jakelujärjestelmään.
     - Ei pääsyä järjestelmänvalvojan työkaluihin tai taloushallinnon tietoihin.
3. **Autentikointi ja valtuutus**
   - Sairaanhoitaja kirjautuu järjestelmään käyttäen monivaiheista autentikointia (MFA), kuten salasanaa ja turvakoodia puhelimeen.
   - Pääsynhallintajärjestelmä tarkistaa sairaanhoitajan tunnistetiedot ja myöntää pääsyn vain niihin resursseihin, joihin hänellä on oikeudet.
4. **Identiteetin hallinta ja valvonta**
   - Sairaanhoitajan toimintaa seurataan jatkuvasti, jotta voidaan varmistaa, ettei hän käytä oikeuksiaan väärin.
   - Kaikki toiminnot kirjataan auditointijälkiin, jotka auttavat varmistamaan säädösten noudattamisen.

jamk

Pääsynhallinta

Esimerkki – Sairaanhoitajan pääsyoikeudet – Haittaohjelman vaikutus

1. **Haittaohjelman laukaisu**
    - Sairaanhoitajan tietokoneelle asennettu haittaohjelma aktivoituu ja yrittää käyttää sairaanhoitajan käyttöoikeuksia päästäkseen käsiksi potilastietoihin ja muihin järjestelmiin.
2. **Pääsynhallinnan suojaus**
    - Pääsynhallintajärjestelmä havaitsee epäilyttävän toiminnan, kuten epätavalliset kirjautumisyritykset tai tiedostojen käsittelyn.
    - Mukautuva autentikointi voi vaatia lisätunnistautumista, kuten biometrisiä tunnisteita, ennen kuin pääsy myönnetään.
3. **Vähimpien oikeuksien periaate**
    - Haittaohjelma ei pääse käsiksi järjestelmänvalvojan työkaluihin tai taloushallinnon tietoihin, koska sairaanhoitajalla ei ole näihin oikeuksia.
    - Pääsynhallintajärjestelmä rajoittaa haittaohjelman toimintaa, koska sairaanhoitajan oikeudet ovat rajatut.
4. **Erityisoikeuksien hallinta**
    - Järjestelmänvalvojien ja muiden korkean käyttöoikeustason käyttäjien tilit on suojattu erityisoikeuksien hallinnan avulla, mikä estää haittaohjelmaa käyttämästä näitä tilejä.
5. **Toimenpiteet**
    - IT-tiimi saa hälytyksen epäilyttävästä toiminnasta ja ryhtyy toimenpiteisiin haittaohjelman poistamiseksi ja tietoturvan palauttamiseksi.

jamk

Pääsynhallinta

Pohdinta

- Miten pääsynhallinta on toteutettu oppilaitoksessa?
  - Fyysiset tilat
  - Loogiset järjestelmät
- Opettajilla ja opiskelijoilla on pääsy oppimisympäristöön (esim. Moodle)
  - Miten tämä pääsy eroaa opiskelijan ja opettajan välillä
- Opettajilla ja opiskelijoilla on pääsy opintorekisterijärjestelmään (esim. Peppi)
  - Opiskelijat näkevät omaa edistymistänsä ja numeroita
  - Opettaja taas voi myöntää omilta opintojaksoiltansa suoritusmerkintöjä
  - Onko muita rooleja?

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

05B – Salasanat ja tunnistautuminen

© 2025 Ovaska Joonatan – Creative Commons 4.0 (CC BY-SA)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Salasanat ja tunnistautuminen

Mikä on salasana?

- Salasana on keino todentaa käyttäjiä salaisen tiedon avulla. Salasana pidetään salassa niiltä, joille salattavan kohteen käyttö ei ole sallittua.
  - Esimerkiksi sodissa on käytetty salasanoja sallimaan pääsy vartiopaikalle vain tietyille henkilöille. Tässä käytössä Suomen puolustusvoimissa puhutaan tunnussanasta.
- Nykyään salasanoja käytetään suojaamaan esimerkiksi tietokonejärjestelmiä, matkapuhelimia, TV-vastaanottimen asetuksia, pankkiautomaatteja ja muita henkilökohtaisia asioita. Nimestään huolimatta salasanan ei tarvitse aina olla sana, vaan se voi myös olla kokonainen lause tai pelkistä numeroista koostuva PIN-koodi.
- Salasana pitää vaihtaa jos tiedetään tai epäillään salasanan joutuneen vääriin käsiin. Lisäksi jos samaa salasanaa on käytetty eri paikoissa myös niissä salasana on vaihdettava.

Lähde: https://fi.wikipedia.org/wiki/Salasana, viitattu 13.11.2024

jamk

Salasanat ja tunnistautuminen

Kuinka valita salasana stand up ☺

- Katsotaanpas kuinka me kaikki valitsimme meidän ensimmäisen salasanan
  - https://www.youtube.com/watch?v=aHaBH4LqGsI
    - Ensimmäiset n. 4 minuuttia

jamk

Salasanat ja tunnistautuminen

Uhat ja turvallisuusnäkökohdat – Autentikointi uhat

- Hyökkääjä, joka saa haltuunsa jonkun käyttämän tunnistautumisvälineen, voi esiintyä kyseisen henkilönä. Tunnistautumisvälineisiin kohdistuvat uhat voidaan jakaa kolmeen ryhmään:
  - **Jotain, mitä tiedät**: Salasana tai PIN-koodi.
  - **Jotain, mitä sinulla on**: Älypuhelin tai turvalaite.
  - **Jotain, mitä olet**: Sormenjälki tai kasvojentunnistus.

Lähde: https://pages.nist.gov/800-63-3/sp800-63b.html, viitattu 14.11.2024

jamk

Salasanat ja tunnistautuminen

Uhat ja turvallisuusnäkökohdat – Tyypillisiä uhkia/hyökkäyksiä, joihin voit vaikuttaa

Hyökkäys/Uhka	Selite	Esimerkki	Lievennysmekanismit
Varkaus	Fyysinen todennuslaite varastetaan	Todennukseen käytettävä laite (esim. matkapuhelin, tunnistekortti, tms.) varastetaan	Käytä monivaiheisia todennustapoja, jotka vaativat muistettavan salaisuuden ja esim. biometrisen tunnisteen
Kopiointi	Todennustieto kopioidaan käyttäjän tietämättä tai tietäen	Paperille tai tiedostoon kirjoitetut salasanat paljastuvat	Käytä todennustietoja, joita on vaikea kopioida tai joihin on vaikea päästä käsiksi
Salakuuntelu, sekä olan yli kurkkiminen	Todennustiedon salaisuus tai tulos paljastuu hyökkääjälle todennuksen aikana	Näppäinpainallusten tarkkailu fyysisessä tilassa tai haitallisella ohjelmistolla	Käytä suojakalvoa näytölle, varmista tilaturvallisuus, päätelaitteen turvallisuus, vältä epäluotettavia langattomia verkkoja
Kalastelu tai huijaus Phishing ja Pharming	Todennustiedon tulos siepataan huijaamalla käyttäjää ajattelemaan, että hän on kirjautumassa oikeaan palveluun	Salasana paljastuu väärennetylle verkkosivustolle	Opi tunnistamaan tyypillisimmät kalasteluun kuuluvat esimerkit, käytä monivaiheista tunnistautumista
Sosiaalinen manipulointi	Hyökkääjä luo luottamusta saadakseen käyttäjän paljastamaan salaisuutensa	Salasana paljastuu kollegalle, joka pyytää sitä pomon puolesta tai puhelimessa tekeytyneenä ylläpitäjäksi	Varmista vastapuolen henkilöllisyys, äläkä ikinä paljasta salasanojasi kenellekään
Online-arvailu	Hyökkääjä yrittää arvata oikean tunnistetiedon tuloksen	Sanakirjahyökkäykset tai raa'an laskentavoiman hyökkäykset muistettuihin salaisuuksiin	Käytä vahvoja yksilöllisiä salasanoja eri palveluihin
Päätelaitteen saastuminen	Haittaohjelma käyttää todennustietoja ilman käyttäjän suostumusta	Haittaohjelma käyttää tai lähettää todennustietoja etähyökkääjille	Käytä laitteistotodennuksia, jotka vaativat fyysisen todennuksen, käytä ajantasaista virustorjuntaohjelmistoa

Salasanat ja tunnistautuminen

Aika salasanan murtamiseen

- Oletetaan, että hyökkääjä on ammattilainen ja hänellä on asiaan sopivan tehokas tietokone ja puolustautumiseen on käytetty asianmukaista salasanan turvaamistekniikkaa.
- Taulukko kuvaa raa'an voiman hyökkäyksiä salasanoja vastaan

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090
Password hash: bcrypt (10)

Hive Systems

Read more and download at hivesystems.com/password

Lähde: https://www.hivesystems.com/password

Salasanat ja tunnistautuminen

Hyvien salasanojen periaatteet

- **Luo vahvoja salasanoja**: Käytä yhdistelmää sanoja, numeroita, symboleja sekä isoja ja pieniä kirjaimia.
- **Vältä helposti arvattavia salasanoja**: Älä käytä esimerkiksi "password" tai "123456".
- **Älä käytä henkilökohtaisia tietoja**: Syntymäpäivät, puhelinnumerot ja perheenjäsenten nimet eivät ole hyviä salasanoja.
- **Käytä pitkiä salasanoja**: Pituus on tärkeämpää kuin monimutkaisuus.
- **Älä käytä samaa salasanaa useissa paikoissa**: Erityisesti älä käytä sähköpostisi salasanaa muilla sivustoilla.
- **Käytä salasanan hallintaohjelmaa**: Ohjelmat kuten LastPass, DashLane ja 1Password voivat auttaa hallitsemaan salasanoja turvallisesti.

Lähde: https://krebsonsecurity.com/password-dos-and-donts/, viitattu 13.11.2024

jamk

Salasanat ja tunnistautuminen

Pohdittavaksi

- Millainen olisi hyvä salasana?
- Kuinka moneen palveluun pystyy pääsemään käsiksi, jos pääpalautussähköpostisiisi päästäisiin käsiksi?
- Miksi haluat käyttää erillisiä sähköpostitilejä ja salasanoja henkilökohtaisiin ja työasioihin?
  - Hyökkääjän kannalta työntekijä sinä saattaa olla mielenkiintoisempi kohde, kuin siviili sinä
- Voitko lisätä monivaiheista tunnistautumista tärkeisiin palveluihin?
- Oletko harkinnut erillisen roskapostin perustamista tai käyttänyt väliaikaisia sähköpostipalveluita?

jamk

Salasanat ja tunnistautuminen

Esimerkki tapaus – Kuvitteellinen sosiaalityöntekijä Anna

- **Salasanat:**
  - **Vahvat salasanat**: Anna käyttää vahvoja ja uniikkeja salasanoja kaikissa työympäristön järjestelmissä, kuten asiakastietojärjestelmässä ja sähköpostissa. Hän käyttää salasanan hallintaohjelmaa, joka auttaa häntä luomaan ja hallitsemaan monimutkaisia salasanoja.
  - **Säännöllinen vaihtaminen**: Anna vaihtaa salasanansa säännöllisesti ja varmistaa, että ne eivät ole helposti arvattavissa.
- **Tunnistautuminen:**
  - **Kaksivaiheinen tunnistautuminen (2FA)**: Anna on ottanut käyttöön kaksivaiheisen tunnistautumisen kaikissa mahdollisissa järjestelmissä. Tämä tarkoittaa, että kirjautuessaan hän käyttää sekä salasanaa että toista tunnistautumismenetelmää, kuten tekstiviestillä saatavaa koodia tai autentikointisovellusta.
  - **Henkilökohtainen ja työelämän erottaminen**: Anna käyttää eri tunnistautumistapoja henkilökohtaisiin ja työasioihin, mikä vähentää riskiä, että henkilökohtaiset tietonsa vaarantuvat työpaikan tietomurron yhteydessä.
- **Pääsynhallinta:**
  - **Roolipohjainen pääsynhallinta**: Annalla on pääsy vain niihin tietoihin ja järjestelmiin, joita hän tarvitsee työtehtäviensä suorittamiseen. Tämä vähentää riskiä, että arkaluontoiset tiedot joutuvat vääriin käsiin.
  - **Säännöllinen tarkistus**: Anna ja hänen tiiminsä tarkistavat säännöllisesti, kenellä on pääsy eri järjestelmiin ja tietoihin, ja päivittävät käyttöoikeuksia tarpeen mukaan.
  - **Tietoturvakoulutus**: Anna osallistuu säännöllisesti tietoturvakoulutuksiin, joissa käsitellään ajankohtaisia uhkia ja parhaita käytänteitä tietoturvan ylläpitämiseksi.

jamk

Biometrinen tunnistauminen

Vaikuttavat operaatiot

- Biometrisiä tunnistautumisia käytetään monissa laitteissa ja pääsynhallinnan elementteinä, joko osana monivaiheista tunnistautumista tai vaihtoehtoiseen tunnistautumiseen.
- Potilas-/asiakastyössä olisi hyvä muistuttaa, myös jos biometrisille tunnisteille tulee muutoksia: Sormenjälki, kasvojentunnistus, iris- ja verkkokalvontunnistus, äänentunnistus.
    - Esim. leikkausoperaatio

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

05C – Tilaturvallisuus

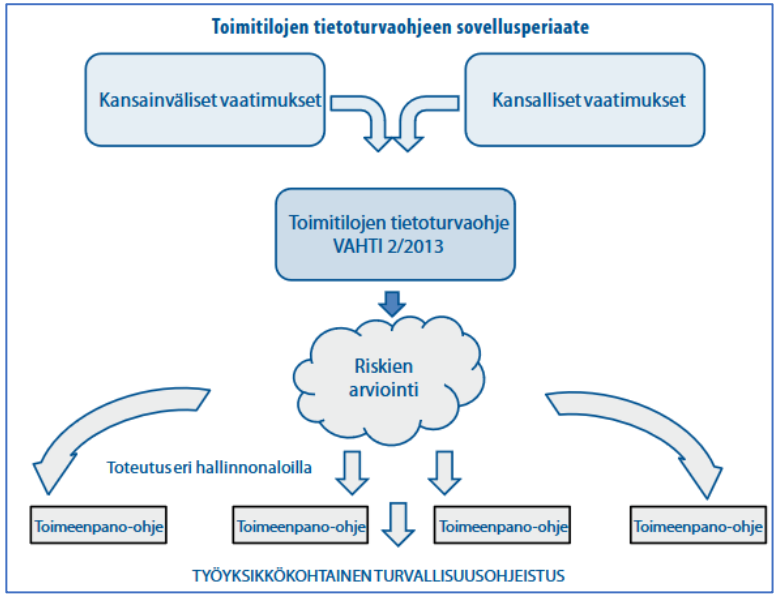
© 2025 Ovaska Joonatan – Creative Commons 4.0 (CC BY-SA)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Tilaturvallisuus

Vahtiohjeistus

- VAHTI-ohjeistukset ovat valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) laatimia ohjeita ja suosituksia, jotka koskevat digitaalista turvallisuutta. Ne kattavat laajasti erilaisia tietoturvaan liittyviä aiheita ja tarjoavat käytännön ohjeita ja parhaita käytäntöjä organisaatioiden tietoturvan parantamiseksi. Ohjeistukset on suunnattu erityisesti julkishallinnon organisaatioille, mutta ne voivat olla hyödyllisiä myös muille toimijoille. VAHTI-ohjeistukset sisältävät muun muassa:
  - Tietoturvapolitiikan kehittämisen ja ylläpidon
  - Riskienhallinnan menetelmiä ja käytäntöjä
  - Toimitilojen turvallisuuden ohjeita
  - Tietojen käsittely ja säilytys
  - Henkilöstön koulutus



Lähde: https://dvv.fi/vahti, VAHTI 2 / 2013

jamk

Tilaturvallisuus

Vahtiohjeistus

- **Pääsynhallinta**: Tilaturvallisuus on keskeinen osa sosiaali- ja terveysalan toimintaa, sillä se varmistaa sekä potilaiden että henkilökunnan turvallisuuden ja suojaa arkaluonteisia tietoja. Tilaturvallisuuden tavoitteena on suojata tilat luvattomalta pääsyltä, varkauksilta, ilkivallalta ja muilta turvallisuusuhkilta.
- **Valvonta ja seuranta**: Valvontakameroiden asentaminen kriittisiin kohtiin, kuten sisäänkäynteihin, tietojenkäsittelytiloihin ja varastoihin, on suositeltavaa. Kulunvalvontatietojen säännöllinen seuranta ja analysointi auttavat havaitsemaan mahdolliset uhat ajoissa. Hälytysjärjestelmät, jotka ilmoittavat epäilyttävästä toiminnasta reaaliajassa, lisäävät tilojen turvallisuutta.
- **Fyysinen suojaus**: Tilojen fyysinen suojaus on tärkeää. Tämä sisältää ovien, ikkunoiden ja muiden sisäänkäyntien vahvistamisen ja lukitsemisen. Turvalukkojen, hälytysjärjestelmien ja turva-aitojen käyttö lisää turvallisuutta. Kriittisten infrastruktuurien, kuten sähkö- ja tietoliikennekaapeleiden, suojaaminen fyysisiltä vahingoilta on myös tärkeää.
- **Henkilöstön koulutus**: Henkilöstön koulutus on keskeinen osa tilaturvallisuutta. Henkilöstön tulee tunnistaa ja raportoida turvallisuusuhkia sekä tuntea hätätilanteiden toimintasuunnitelmat. Säännölliset harjoitukset ja päivitykset turvallisuuskäytännöistä varmistavat, että henkilöstö osaa toimia oikein eri tilanteissa.

Lähde: https://dvv.fi/vahti, VAHTI 2 / 2013

jamk

Tilaturvallisuus

Vahtiohjeistus

- **Tietojen Käsittely ja Säilytys**: Arkaluonteisten tietojen käsittely ja säilytys vaativat erityistä huomiota. Tiedot tulee säilyttää lukituissa kaapeissa tai suojatuissa tietojärjestelmissä, ja pääsy tietoihin tulee rajoittaa vain niille, joilla on siihen oikeus. Salausmenetelmien käyttö tietojen suojaamiseksi siirron ja säilytyksen aikana on suositeltavaa.
- **Hätätilanteiden Hallinta**: Hätätilanteiden hallintasuunnitelmien kehittäminen ja harjoittelu ovat tärkeitä. Evakuointisuunnitelmat ja hätäviestintäjärjestelmät varmistavat, että henkilöstö ja potilaat tietävät, miten toimia hätätilanteissa. Hätäuloskäyntien ja -reittien selkeä merkitseminen ja esteettömyys ovat myös olennaisia.

Soveltaminen sosiaali- ja terveydenhuollossa

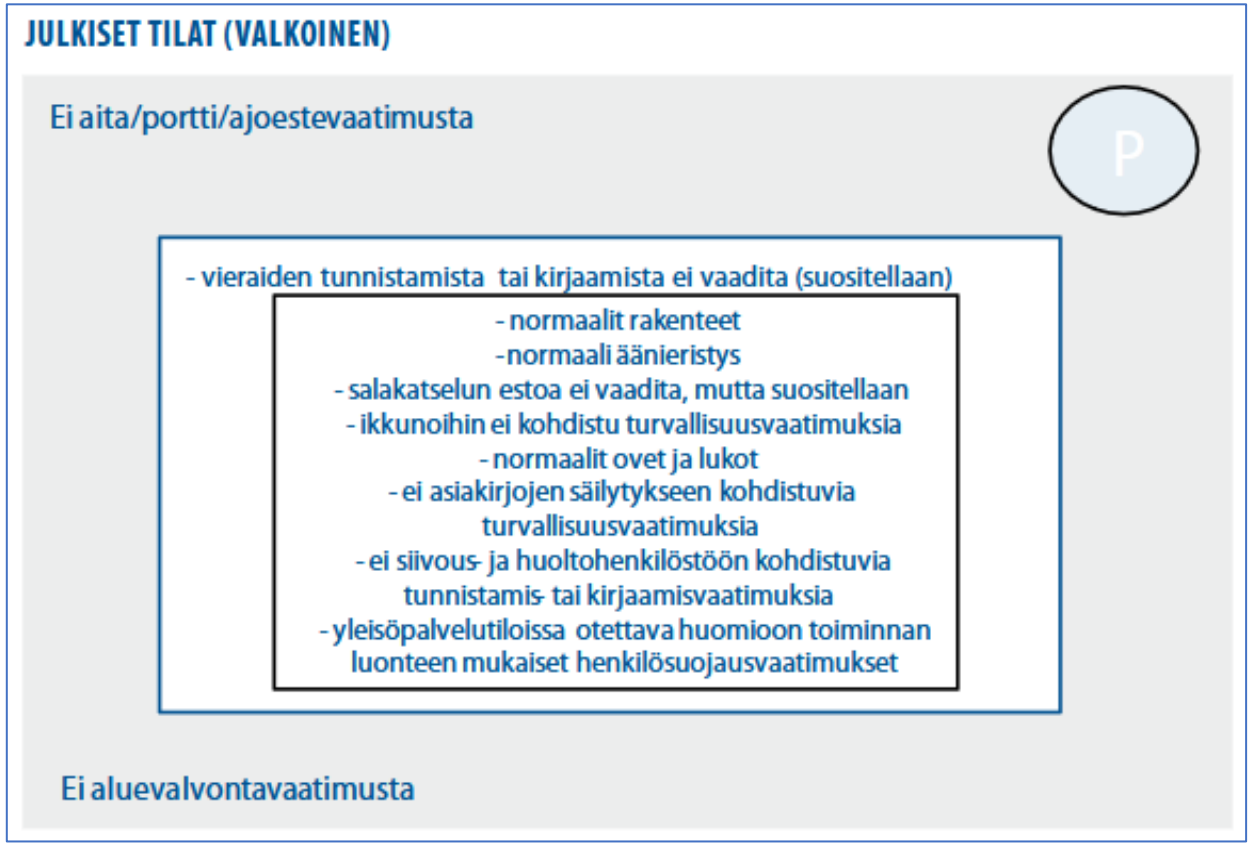
- Sosiaali- ja terveysalalla tilaturvallisuus on erityisen tärkeää potilastietojen suojaamiseksi ja potilaiden turvallisuuden varmistamiseksi. Tämä tarkoittaa käytännössä potilastietojen turvallista säilytystä ja käsittelyä, hoitotilojen fyysistä suojausta sekä hätätilanteiden hallintasuunnitelmien kehittämistä ja harjoittelua.

Lähde: https://dvv.fi/vahti, VAHTI 2 / 2013

jamk

Tilaturvallisuus

Vahtiohjeistuksen esimerkki julkisesta tilasta

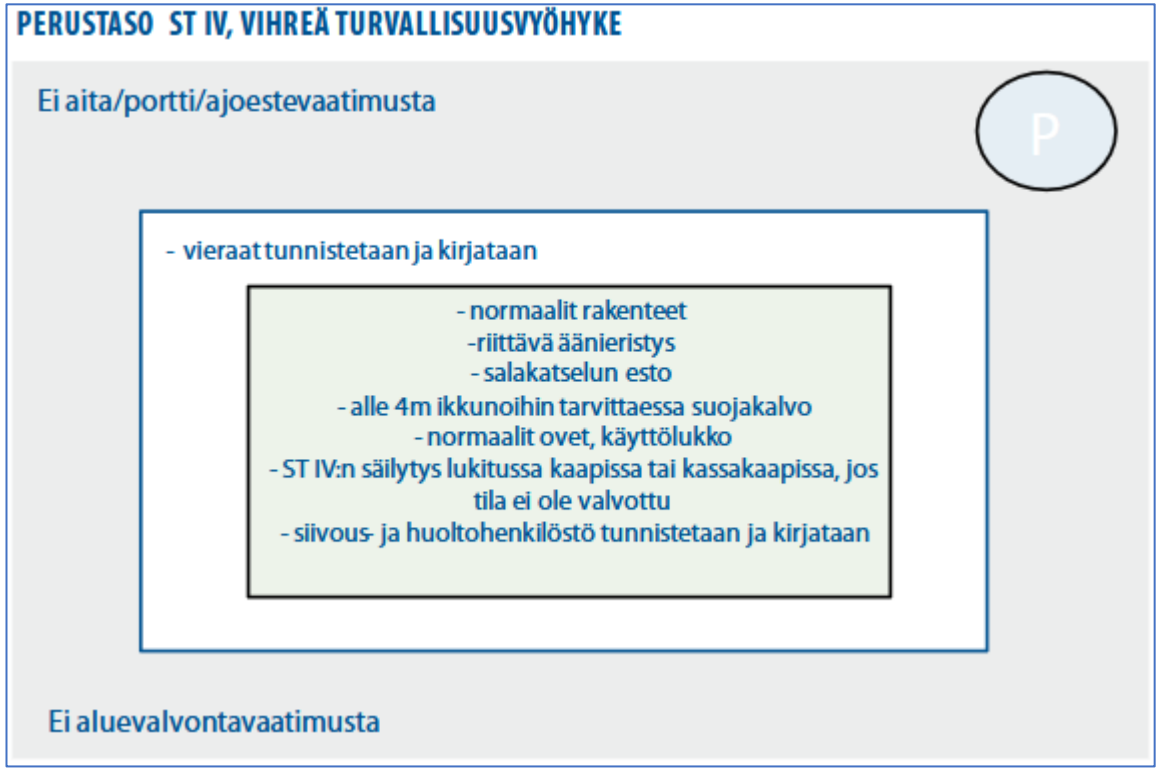


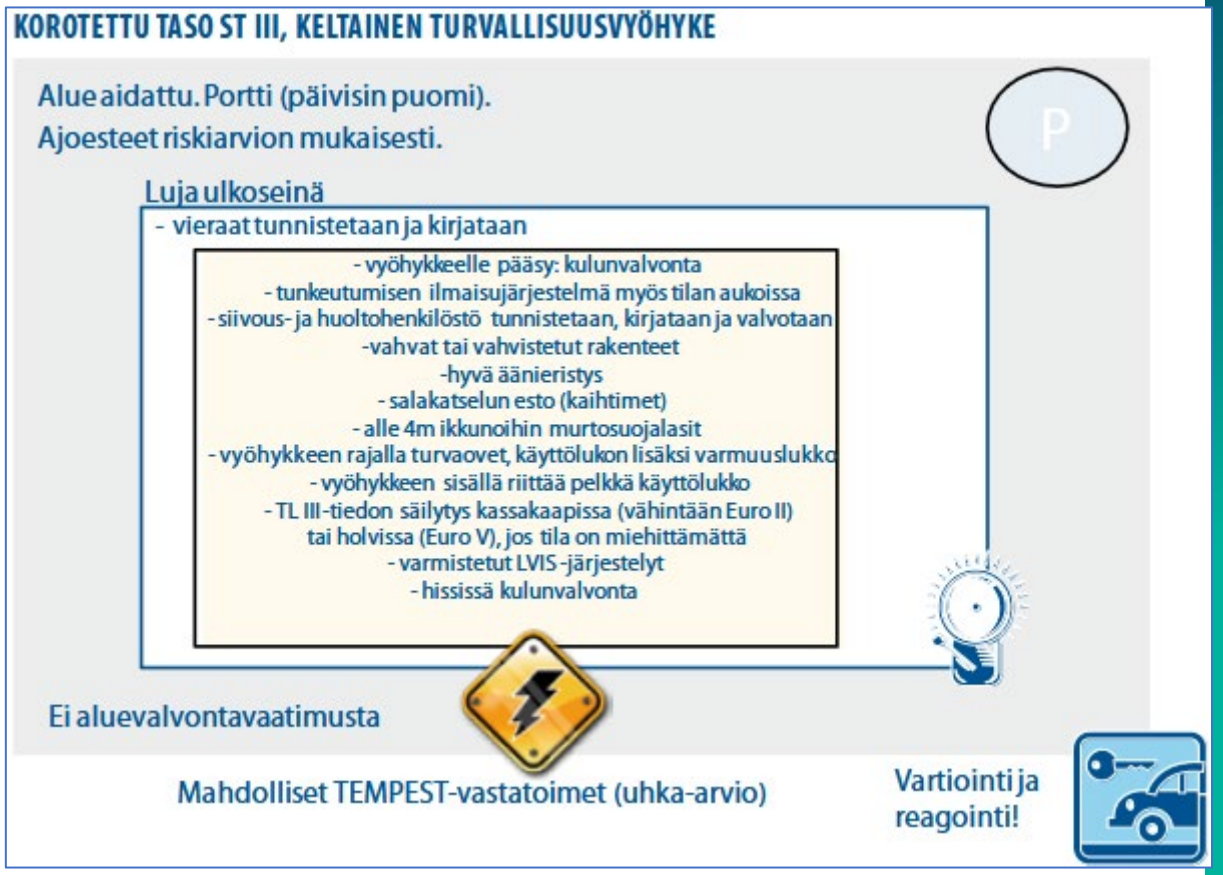
Lähde: https://dvv.fi/vahti, VAHTI 2 / 2013, ISBN 978-952-251-461-5 (PDF)

jamk

Tilaturvallisuus

Vahtiohjeistuksen esimerkki suojatasoista 3 ja 4





Lähde: https://dvv.fi/vahti, VAHTI 2 / 2013, ISBN 978-952-251-461-5 (PDF)

Fyysinen tietoturva

- Fyysinen tietoturva tarkoittaa toimenpiteitä, joilla suojataan organisaation tärkeät tiedot fyysisiltä uhilta.
- Tässä ovat keskeiset elementit lyhyesti:
  - **Tilojen suunnittelu ja rakenteet**: Tiedon käsittely- ja säilytystilat suojataan fyysisillä rakenteilla, kuten seinillä, lukituilla ovilla ja näkösuojilla
  - **Turvallisuusjärjestelmät**: Käytetään kameravalvontaa, hälytysjärjestelmiä, kulunvalvontaa ja lukitusjärjestelmiä estämään luvaton pääsy
  - **Henkilöstön rooli**: Henkilöstön koulutus ja sitoutuminen tietoturvakäytäntöihin on olennaista. Tämä sisältää esimerkiksi "puhdas pöytä" -periaatteen noudattamisen ja työasemien lukitsemisen.
  - **Riskiarvioinnit**: Säännölliset riskiarvioinnit auttavat tunnistamaan ja hallitsemaan fyysisiä uhkia, kuten tulipaloja, vesivahinkoja ja varkauksia.
  - **Turva-alueet**: Määritellään erilliset turva-alueet, joissa on tiukemmat suojatoimenpiteet, kuten palvelinkeskukset.
  - **Olosuhteilta suojautuminen**: Suojatoimenpiteet tulipaloja, vesivahinkoja ja sähkökatkoja vastaan, kuten paloilmaisimet ja varavirtalähteet.

Lähde: https://www.savelan.fi/mita-on-fyysinen-tietoturva/, viitattu 19.11.2024

jamk

Fyysinen tietoturva

Kuvitteellinen sosiaalitoimisto "Hyvinvointikeskus", jossa sosiaalityöntekijä Laura työskentelee.

- **Lukitut toimistotilat**: Lauran työhuone on lukittu aina, kun hän ei ole paikalla. Tämä estää luvattoman pääsyn asiakastietoihin.
- **Näkösuojat**: Lauran työpöydällä on näkösuojat, jotka estävät asiakkaita tai vierailijoita näkemästä tietokoneen näyttöä tai asiakirjoja.
- **Kameravalvonta**: Hyvinvointikeskuksen sisäänkäynnit ja käytävät ovat kameravalvonnassa, mikä lisää turvallisuutta ja estää luvattoman pääsyn.
- **Hälytysjärjestelmät**: Toimistossa on hälytysjärjestelmä, joka aktivoituu työajan ulkopuolella ja ilmoittaa mahdollisista murtautumisyrityksistä.
- **Tietoturvakoulutus**: Laura ja hänen kollegansa osallistuvat säännöllisesti tietoturvakoulutuksiin.
- **Puhdas pöytä -periaate**: Laura noudattaa "puhdas pöytä" -periaatetta, eli hän ei jätä asiakirjoja tai muistilappuja työpöydälleen päivän päätteeksi.
- **Säännölliset tarkastukset**: Hyvinvointikeskuksessa tehdään säännöllisiä riskiarviointeja, joissa tarkastetaan fyysisen tietoturvan taso ja tehdään tarvittavat parannukset.
- **Arkistohuone**: Asiakastietoja säilytetään lukitussa arkistohuoneessa, johon on pääsy vain valtuutetuilla työntekijöillä.
- **Paloilmaisimet ja sammutusjärjestelmät**: Toimistossa on paloilmaisimet ja automaattiset sammutusjärjestelmät, jotka suojaavat asiakirjoja.
- **Varavirtalähteet**: Tärkeät tietokoneet ja palvelimet on kytketty varavirtalähteisiin, jotka takaavat toiminnan jatkuvuuden sähkökatkon aikana.

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

05D – Yhteenveto

© 2025 Ovaska Joonatan – Creative Commons 4.0 (CC BY-SA)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Yhteenveto

Valtuudet

- Ammatti/työnkuva/työpiste kohtaisesti voidaan määritellä esim. mihin potilaan sairaskertomustietojen sisältöihin tai näkymiin sinulla tai siis sinun käyttäjätunnuksillasi/resurssillasi on pääsyoikeus. Perustellusti näihin sitten voi hakea muutosta.
    - Esimerkki käytännöstä: Sinulla ei ollut sairaanhoitajana päivystysalueella toimiessasi tunnuksillasi oikeutta nähdä potilaan mielenterveys-päihdepuolen sairaskertomusnäkymiä eli kirjauksia, mutta kuitenkin työnkuvaasi kuului kyseisen potilasryhmän hoito ja säännöllinen lääkitseminen päivystyksessä. Hoitosuunnitelma, lääkemääräykset/ohjeistukset yms. olivat kuitenkin nähtävissä vain mielenterveys- ja päihdepuolen ammattilaisten kirjauksissa. Näin ollen potilasturvallisuuden ja hoidon jatkuvuuden vuoksi sairaanhoitajan käyttöoikeuksia sairaskertomusnäkymiin lisättiin näiltä osin, jotta päivystyksessä päästiin toteuttamaan turvallisesti potilaan hoito sekä lääkitseminen.

jamk

Yhteenveto

Valtuudet

- Tietyillä ammattilaisilla on työnkuvansa vaatimusten ja vastuualueensa mukaisesti luotu laajemmat käyttöoikeudet työyksikössä esim. potilastietojärjestelmän käyttöoikeuksiin tai joidenkin osa-alueiden muokkaamiseen. Esim. ajanvarausjärjestelmät, käyttöoikeuksien lukitustilojen resetointi/avaaminen tms.
- Esimerkkinä käyttäjätunnuksiin liittyen:
  - Tunnuksillasi avaat vain oman koneen ja omat ohjelmat etkä anna muiden kirjata tai toimia koneella tunnuksillasi. Käytännössä ongelmia saattaa kuitenkin tulla, jos vaikkapa viikonloppuna ei keikkailijan (lääkäri, sairaanhoitaja jne.) tunnukset koneen aukaisuun toimikaan ja työt olisi ehdottomasti saatava alkamaan. Saattaa olla, että kone aukaistaan vuorossa olevan tunnuksilla ja keikkailija itse sitten pääsisikin kirjautumaan potilastietojärjestelmään. Silti hän on toisen henkilön käyttäjätunnuksilla koneelle kirjautuneena ja voi hänen nimissään seikkailla sivustoilla, päästä kenties sähköpostiin, Teamsiin jne....
  - Harjoittelujaksoja tekevillä opiskelijalla on kirjaamisen ja pääsynsuhteen pienemmät oikeudet, kuin rekisteröidyillä työntekijöillä

jamk

Yhteenveto

Auditointijäljet eli “lokitiedot”

- Mm. kaikista potilastietoihin kirjautumisista jää merkinnät eli käyttäjän “sormenjäljet”, joita organisaatio omien ohjeistuksiensa mukaisesti seuraa.
- Säännönmukaisesti tehdään tarkistuksia ja jos huomataan, että olet esim. käynyt omissa tiedoissasi, niin asia otetaan selvitykseen.
- Asiakkaalla/potilaalla on oikeus saada nähdä omien potilastietojensa lokimerkinnät.

jamk

Yhteenveto

Fyysiset tilat

- Vaikka henkilökunnalla on kulkukortit/henkilöllisyyskortit, on siltikin hyvin mahdollista, että ulkopuolinen henkilö pääsee tiloihin sisään vaikkapa samalla oven avauksella kuin henkilökunnankin jäsen.
- Asiakkaat/potilaat saapuvat kutsuttuna vastaanottohuoneeseen, josta ammattilainen hetkeksi poistuu konsultoimaan, hakemaan välineitä, hakemaan tulosteen printteristä tms., jolloin asiakkaalla on mahdollisuus koneen jäädessä auki tai ammattilaiskortin jäädessä koneeseen päästä koneelle ja samalla muihin tietoihin käsiksi. Tai sinulla jää kone auki huoneeseesi, jossa päivän potilaslista esillä tulosyineen, poistut hetkeksi ja kollega käyttää hetken huonettasi tutkiessa omaa asiakastaan. Sinun tunnuksillasi oleva kone ja useat asiakastiedot ovat esillä ulkopuolisille.
- Myös sosiaali- ja terveysalalla on työskentelytiloina avoimia tiloja ja konttoreita, jolloin jollakin henkilöllä on mahdollisuus nähdä ja päästä käsiksi sinun työkoneeseesi tai nähdä salasanat tms. Koneen auki jättäminen, vaikka vain hetkeksi poistuisit paikalta, on hyvin yleistä.
- Henkilötietoja sisältäviä papereita/tulosteita (sähköisten reseptien paperiohje, laboratoriotuloksia, EKG-nauhoja) edelleen on paperiversioina, jotka eivät saa jäädä pöydille tai tavallisiin roskakoreihin --> TIETOSUOJAROSKAKORI

jamk

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences