TIETOTURVAOHJE

Johanna Hakonen

Sisällysluettelo

1 Johdanto

Asiakasyritys on fiktiivinen fysioterapiakeskus Physio, jonka hoitohenkilökunnan määrä on viisi ja tietohallinnosta vastaa yksi henkilö. IT-ympäristö sisältää Windows-palvelimen ja -työasemia ja Active Directoryn. Yrityksellä on Physio-verkkosivut ajanvarausta varten ja Kanta-palveluun liitetty potilastietojärjestelmä. Tietoturvaohjeen teossa käytettiin Kyberturvallisuuskeskuksen Pienyritysten kyberturvallisuusopasta (Kyberturvallisuuskeskus, 2025) ja ChatGPT:tä (OpenAI, 2025).

2 Tietoturvaohje

2.1 Laitteiden ja ohjelmistojen käyttö

Käytä vain yrityksen hyväksymiä laitteita ja ohjelmistoja työtehtävissä.

Lukitse tietokone aina poistuessasi työpisteeltä (Win + L).

Päivitysten asennuksesta ja varmuuskopioinnista ei tarvitse huolehtia, vaan ne hoituvat automaattisesti.

2.2 Salasanat ja tunnistautuminen

Käytä vahvoja salasanoja, mieluiten salalauseita, äläkä jaa niitä kenellekään. Edes järjestelmän ylläpitäjän tai perheenjäsentesi ei tarvitse tietää salasanaasi.

Salasana vaihdetaan 30 päivän välein. Käytä kaikissa palveluissa eri salasanaa.

Meillä käytetään salasanan tallennukseen Bitwarden-ohjelmaa ja monivaiheista tunnistautumista (Windows Hello).

2.3 Asiakastiedot ja tietosuoja

Käsittele asiakastietoja vain työtehtävien vaatimalla tavalla.

Älä jätä asiakas- tai potilastietoja näkyville.

Älä käsittele asiakastietoja suojaamattomilla laitteilla tai henkilökohtaisilla sähköpostitileillä.

2.4 Sähköposti ja tietojenkalastelu

Älä avaa epäilyttäviä sähköposteja tai linkkejä. Jos saat linkin palveluntarjoajalta ja pyynnön kirjautua sivuille nopeasti, suosittelemme lähetetyn linkin sijaan kirjautumaan palveluntarjoajan oman verkkosivun kautta ja siten varmistamaan, onko viesti aito.

Jos saat epäilyttävän viestin, ilmoita IT-tuelle.

Varmista lähettäjän aitous ennen liitetiedostojen avaamista. Jos et ole varma vastaanottamasi viestin lähettäjästä tai sen sisällöstä, varmista asia esimerkiksi soittamalla viestin lähettäjälle. Katso yhteystiedot muualta kuin lähetetystä viestistä (esim. virallisilta verkkosivuilta).

2.5 Fyysinen tietoturva

Älä jätä työasemia tai asiakastietoja valvomatta.

Vierailijat eivät saa käyttää yrityksen tietokoneita.

Säilytä arkaluontoiset asiakirjat lukitussa tilassa.

2.6 Tietoturvaloukkauksista ilmoittaminen

Ilmoita IT-tuelle kaikista tietoturvaan liittyvistä epäilyistä tai häiriöistä.

Nopeasti havaittu ja ilmoitettu uhka vähentää vahinkoja.

2.7 Tietoturva kehittyy jatkuvasti

Osallistu säännöllisiin tietoturvakoulutuksiin.

Pysy ajan tasalla uusista tietoturvakäytännöistä.

Lähdeluettelo

Kyberturvallisuuskeskus. (23. Maaliskuu 2025). *Pienyritysten kyberturvallisuusopas*. Noudettu osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

OpenAI. (17. Maaliskuu 2025). *ChatGPT*. Noudettu osoitteesta chatgpt.com