

TÄISKASVANUTE TÄIENDUSKOOLITUSE ÕPPEKAVA

1. Üldandmed

Õppeasutus:	Valgamaa Kutseõppekeskus
Õppekava nimetus: (venekeelsetel kursustel nii eesti kui vene keeles):	Turvaline digikäitumine ja küberturbe ennetus töökohtadel
Õppekavarühm: (täiendus- koolituse standardi järgi)	Arvutikasutus
Õppekeel:	eesti keel

2. Koolituse sihtgrupp ja õpiväljundid

Sihtrühm ja selle kirjeldus ning õppe alustamise nõuded. Ära märkida milliste erialaasukste, haridustaseme või vanusegrupi inimestele koolitus on mõeldud ning milline on optimaalne grupi suurus; ära tuua kas ja millised on nõuded õpingute alustamiseks.

Koolitus on mõeldud ettevõtete töötajatele, kes igapäevaselt kasutavad arvutit, e-posti või muid digilahendusi ning vajavad teadmisi turvalisest digikäitumisest ja küberturberiskide ennetamisest.

Sihtrühma kuuluvad: kontoritöötajad, teenindustöötajad, juhid, väikeettevõtete töötajad ja kõik teised ettevõtete töötajad, kelle tööks on arvuti või nutiseadmete kasutamine.

Optimaalne grupi suurus: 10 õppijat.

Õppe alustamise nõuded

- õppija oskab kasutada arvutit ja nutiseadmeid igapäevaste tööülesannete täitmiseks;
- valmidus järgida infoturbe- ja tööohutuse nõudeid;
- tasemeõppes õppijad sihtühma ei kuulu.

Õpiväljundid. Õpiväljundid kirjeldatakse kompetentsidena, mis täpsustavad, millised teadmised, oskused ja hoiakud peab õppija omandama õppeprotsessi lõpuks.

Koolituse lõpuks õppija:

1. **Selgitab** küberturvalisuse põhimõtteid, levinumaid ohte ja ettevõtetele mõjuvaid küberturberiske.
2. **Tuvastab** pahatahtlikud e-kirjad, pettused, ebaturvalised veebilehed ja sotsiaalse manipuleerimise võtted.
3. **Kasutab** turvalist paroolihaldust, mitmeastmelist autentimist ja turvalisi digivõtteid igapäevases töös.
4. **Rakendab** turvalist käitumist seadmete, failide ja ettevõtte andmete kaitsmisel.
5. **Analüüsib** oma töökoha küberturbe taset ning teeb põhjendatud ettepanekuid riskide vähendamiseks.
6. **Tegutseb** küberturbe intsidenti kahtlustades vastavalt juhiste ja oskab sellest korrektselt teatada.

Õpiväljundite seos kutsestandardi või tasemeõppe õppekavaga. Tuua ära vastav kutsestandard ning numbriline viide konkreetsetele kompetentsidele, mida saavutatakse.

Koolitus toetab täiskasvanute digipädevuste arendamist ning on kooskõlas Euroopa

Digipädevusraamistiku DigComp 2.2 kompetentsidega, mis on aluseks ka Eesti tasemeõppe digipädevuste nõuetele.

Õpiväljundid on seotud järgmiste DigComp kompetentsidega:

DigComp valdkond 1: Informatsiooni ja andmete kirjaoskus

- 1.2 – info hindamine (ohtlike, eksitavate ja pahatahtlike sõnumite tuvastamine)
- 1.3 – teabe haldamine turvaliselt

DigComp valdkond 2: Kommunikatsioon ja koostöö

- 2.4 – netikett ja turvaline suhtlus digikeskkonnas
- 2.5 – isikuandmete kaitse ja privaatsus

DigComp valdkond 4: Turvalisus

- 4.1 – seadmete ja sisu kaitsmine
- 4.2 – isikuandmete ja privaatsuse kaitse
- 4.3 – tervise ja heaolu tagamine digikeskkonnas
- 4.4 – keskkonnamõju arvestamine digiseadmete kasutamisel

DigComp valdkond 5: Probleemilahendus

- 5.1 – tehniliste probleemide lahendamine
- 5.3 – vajaduspõhine uute turvaliste lahenduste valik

Koolitus toetab ka tasemeõppe **“Infosüsteemide arendus”, “IT-süsteemide haldus”** ja **“Noorem tarkvara-arendaja”** õppekavade digiturbe mooduleid, andes õppijatele oskusi, mida kasutatakse igapäevases töökeskkonnas: turvaline digikäitumine, riskide vältimine, andmete kaitsmine ja küberturvalisuse põhimõtete järgimine.

Põhjendus. *Tuua põhjendus koolituse sihtrühma ja õpiväljundite valiku osas.*

Koolitus on suunatud ettevõtete töötajatele, kelle igapäevatöös on vältimatu arvuti, nutiseadmete ja digikeskkondade kasutamine. Tööandjate hinnangul on kasvav vajadus selliste töötajate järele, kes suudavad märgata küberturbeohte, vältida andmeleketega seotud riske ning tagada ettevõtte andmete ja tööprotsesside turvalisus. Küberturvalisus on osa kaasaegsest organisatsiooni jätkusuutlikkusest ning mõjutab otseselt tööprotsesside tõhusust ja töökatkestuste vältimist.

Õpiväljundid on valitud selliselt, et need toetavad õppija praktilisi oskusi riskide tuvastamisel, turvalisel digikäitumisel, paroolihaldusel, seadmete kaitsmisel ja intsidentidele reageerimisel. Need oskused on vajalikud kõigis organisatsioonides sõltumata töösuundadest ning aitavad töötajatel vähendada küberturberiske, mis ohustavad nii ettevõtte tegevust kui ka teenuste järjepidevust.

3. Koolituse maht

Koolituse kogumaht akadeemilistes tundides:	24
Kontaktõppe maht akadeemilistes tundides:	24
sh auditoorse töö maht akadeemilistes tundides: (õpe loengu, seminari või muus koolis määratud vormis)	14
sh praktilise töö maht akadeemilistes tundides: (õpitud teadmiste ja oskuste rakendamine õppekeskkonnas)	10

4. Koolituse sisu ja õppekeskkonna kirjeldus ning lõpetamise nõuded

Õppe sisu ja õppekeskkonna kirjeldus. *Tuua peamised teemad ja alateemad sh eristada auditoorne ja praktiline osa. Esitada õppekeskkonna lühikirjeldus, mis on õpiväljundite saavutamiseks olemas. Loetleda kursuse kohustuslikud õppematerjalid (nt õpikud vmt) kui need on olemas. Kui õppijalt nõutakse mingeid isiklikke õppevahendeid, tuua ka need välja.*

Auditoorne osa (14 akadeemilist tundi)

- Küberturvalisuse põhimõtted ja levinumad ohud
- Sotsiaalne manipuleerimine (phishing, scam, petukõned)
- Paroolihaldus ja mitmeastmeline autentimine
- Turvaline e-post ja veebikäitumine
- Andmete kaitse ja isikuandmete turvaline käitlemine
- Seadmete ja võrkude turvaline kasutamine töökohtadel
- Turvaintsidentide ennetamine ja reageerimise põhimõtted
- Ettevõtte küberturbepoliitika ja töötaja roll selles

Praktiline osa (10 akadeemilist tundi)

- Pahatahtlike e-kirjade tuvastamine (phishing-treening)
- Turvaliste paroolide loomine ja paroolihalduri kasutamine
- Seadmete turvaseadete läbimine (telefon, sülearvuti)
- Veebilehtede turvalisuse kontrollimise harjutused
- Praktilised juhtumiuuringud (reaalelulised küberintsidendid)
- Rännaku simulatsioon: kuidas ära tunda kahtlane tegevus
- Andmete kaitsmine: failide krüptimine, turvaline jagamine
- Küberturbe ennetusplaani loomine oma töökohta jaoks

Õppekeskkonna kirjeldus

Õpe toimub Valgamaa Kutseõppekeskuse arvutiklassis ja/või seminariruumis, kus on:

- igale õppijale töökoht arvuti või sülearvutiga;
- turvaline internetiühendus ja B-kaabliga võrk;
- projektor või ekraan praktiliste näidete esitamiseks;
- võimalus kasutada paroolihaldureid, turvaseadeid ja simulatsioonikeskkondi;
- keskkond, mis võimaldab küberturberiske turvaliselt simuleerida ja õppida.

Keskkond toetab täielikult kursuse õpiväljundite saavutamist.

Kohustuslikud õppematerjalid

- Koolitaja koostatud juhendmaterjalid ja töölehed
- Küberturbe praktiliste harjutuste komplekt
- Turvalise paroolihalduse ja phishing-tuvastuse juhendmaterjal

Õppijalt nõutavad isiklikud vahendid

- isiklik sülearvuti või tööarvuti (soovituslik, mitte kohustuslik);
- nutitelefon mitmeastmelise autentimise harjutuste jaoks;
- märkmik või digitaalne seade märkmete tegemiseks.

Nõuded õppe lõpetamiseks, sh hindamismeetodid ja –kriteeriumid. *Kirjeldada, kuidas hinnatakse õpiväljundite saavutamist.*

Õppe lõpetamise eelduseks on aktiivne osalus õppetöös ja aruteludes ning kõigi ette nähtud praktiliste ülesannete sooritamine. Õpiväljundite saavutamist hinnatakse praktiliste harjutuste, juhtumianalüüside ja lõpliku küberturbe ennetusplaani esitamise kaudu.

Hindamismeetodid ja hindamiskriteeriumid

1. Praktiline harjutus – pahatahtlike e-kirjade ja ohtlike olukordade tuvastamine

Hindamiskriteeriumid:

- tuvastab phishing'u ja muude ründevormide tunnuseid;
- põhjendab, miks konkreetne sõnum või tegevus on ohtlik;
- teeb turvalise valiku ja väldib riskikäitumist.

2. Paroolihalduse ja seadmete turvaseadete praktiline ülesanne

Hindamiskriteeriumid:

- loob tugeva parooli vastavalt nõuetele;
- kasutab paroolihaldurit ja mitmeastmelist autentimist;
- seadistab seadme põhiturbesätteid korrektselt.

3. Küberturbe ennetusplaani koostamine

Hindamiskriteeriumid:

- analüüsib oma töökoha digiriske;
- teeb realistlikke ettepanekuid riskide vähendamiseks;
- kirjeldab praktilisi samme andmete ja seadmete kaitsmiseks;
- seob oma ettepanekud küberturbe põhimõtetega.

4. Osalemine aruteludes ja juhendatud tegevustes

Hindamiskriteeriumid:

- järgib turvalise digikäitumise juhiseid;
- panustab õppeprotsessi ja sooritab ülesanded korrektselt.

Õppijale väljastatakse tunnistus, kui ta on täitnud lõpetamise tingimused ning saavutanud õpiväljundid nõutud tasemel.

5. Koolitaja andmed

Koolitaja andmed. *Tuua ära koolitaja(te) ees- ja perenimi ning kursuse läbiviimiseks vajalikku kompetentsust näitav kvalifikatsioon või vastav õpi- või töökogemuse kirjeldus.*

Maris Rõõm

Küberturbe ja digiturvalisuse valdkonna koolitaja, kellel on praktiline kogemus turvalise digikäitumise, infoturbe põhimõtete ja riskide ennetamise õpetamisel. Töötanud nii ettevõtete töötajate kui ka täiskasvanute koolitamisel.

Õppekava koostaja:

/ees- ja perenimi, amet, e-mail/

Kaidi Loos

Õpetaja / täiendkoolituse spetsialist

Kaidi.loos@vkok.ee