Kinnitatud Paprika OÜ poolt 23.05.2024

1	Õppekava kinnitamise kuupäev ja number:	23.05.2024
2.	Õppekava nimetus:	Küberturvalisuse ja andmekaitse koolitus kontoritöötajatele
3.	Õppekava koostamise alus:	Kliendi tellimus
4.	Õppekavarühm:	Informatsiooni- ja kommunikatsioonitehnoloogiad
5.	Üldeesmärk:	Kursuse läbinu oskab tunda ära küberohte ja teab nendega võitlemise meetoteid. Kursuse läbinu tunneb andmekaitse aluseid ja rakendab omandatud teadmisi igapäevases töös isikuandmete töötlemisel., saab ülevaate isikuandmete kaitse õiguslikest sätetest ELis ja andmete vahetusest kolmandate riikidega sh Ameerika Ühendriikidega ning arendab praktilisi oskusi ennetamiseks ja tegutsemiseks pahavara rünnakute korral ja oskab kaitsta oma töökohta.
6.	Sihtgrupp:	Sihtrühm on kontoritöötajad, kes kasutavad igapäevaselt arvuteid ja internetti ning töötavad isikuandmetega
7.	Ülevaade protsessist tervikuna, Õppe kogumaht ja ülesehitus, sh. auditoorse, praktilise ja iseseisva töö osakaal;	Kursuse maht on 26 akadeemilist tundi, neist 16 ak t on auditoorne õpe ja 10 ak t on iseseisev töö
8	Õppekeskkond ja -vahendid:	veebikeskkond Zoomis, kuni 20 inimest grupp, õppevahendina on sülearvuti olemasolu.

11. Õpiväljund	Õppe sisu / Teemad	Koolitusmeetodid ja õppevormid	Maht ak. tundides
Tunneb peamisi küberohtusid, nende tekkepõhjuseid ja potentsiaalset mõju	Küberturvalisuse alused Isiklik küberhügieen ja töötaja isiklik vastutus ettevõtte ees, kujuteldavad ja tegelikud ohud, VPN-i	Ülal mainitud õpiväljundite saavutamiseks ja teadmiste omandamiseks kasutatakse koolituse	4

organisatsioonidele	riskid. Milliseid paroole valida ja kuidas neid hoida Küberohtude tüübid ja põhimõtted kasutaja kaitseks ettevõtte e-posti ja krediitkaartide osas	jooksul järgmisi õppemeetodeid: - praktilised harjutused - arutelud - individuaalsed tööd - grupitööd - harjutused ja testid spetsiaalselt välja töötatud õppeplatvormil Kõik õppijad saavad jaotusmaterjalid elektroonilisel kujul.	
Ennetab ja reageerib pahavara rünnakutele, kasutades selleks asjakohaseid tööriistu ja tehnikaid	Infosüsteemide kaitsmise põhimõtted ettevõtetes, turvaportokollid ja –standardid. Riskide haldus ja leevendamise meetmed. Inimestega manipuleerimine (Social engineering), info tõepärasus ja kontrollimine. Andmete krüpteerimine: nii kohalikes kui ka kaughadustes. Turvaliste võrguühenduste loomise ja hooldamise alused, sealhulgas VPN ja Wi-Fi võrkude kaitse. Juurdepääsu haldamise poliitika ja meetodid teabele ja ressurssidele, mitmefaktoriline autentimine.	Ülal mainitud õpiväljundite saavutamiseks ja teadmiste omandamiseks kasutatakse koolituse jooksul järgmisi õppemeetodeid: - praktilised harjutused - arutelud - individuaalsed tööd - grupitööd - kogu koolituse vältel personaalse projekti juhtimine - harjutused ja testid spetsiaalselt välja töötatud õppeplatvormil Kõik õppijad saavad jaotusmaterjalid kas või elektroonilisel kujul.	4
Juhindub oma tegevustes kehtivatest andmekaitse	Euroopa liidu ja Eesti regulatsioon – andmekaitse põhialused ja andmete töötlemise turvalisuse nõuded;	Ülal mainitud õpiväljundite saavutamiseks ja teadmiste omandamiseks kasutatakse koolituse	4

seadustest ja regulatsioonidest	vastutus nõuete mittetäitmise eest, andmete vahetamine kolmandate riikide sh USA-ga. Kohustused ja õigused: andmesubjektide õigused ning andmetöötlejate ja -valdajate kohustused. - Diskussioon tehisintellekti mõjust ühiskonnale: eetiliste põhimõtete ja standardite rakendamine tehisintellekti projektides, et tagada õiglane ja vastutustundlik kasutamine. .	jooksul järgmisi õppemeetodeid: - praktilised harjutused - arutelud - individuaalsed tööd - grupitööd - kogu koolituse vältel personaalse projekti juhtimine - harjutused ja testid spetsiaalselt välja töötatud õppeplatvormil Kõik õppijad saavad jaotusmaterjalid kas paberil või elektroonilisel kujul.	
Hindab küberturvalisuse riske ja rakendab ohutasemele sobivaid riskivältimismeetmeid.	Praktikum: küberkaitse rakendamine ja taastumisstsenaariumid Haavatavuste hindamise meetodid ja intsidentidele reageerimise plaanide väljatöötamine.	Ülal mainitud õpiväljundite saavutamiseks ja teadmiste omandamiseks kasutatakse koolituse jooksul järgmisi õppemeetodeid: - praktilised harjutused - arutelud - kogu koolituse vältel personaalse projekti juhtimine - harjutused ja testid spetsiaalselt välja töötatud õppeplatvormil Kõik õppijad saavad jaotusmaterjalid kas paberil või elektroonilisel kujul.	4

12. Kasutatavad õppematerjalid

Koolitaja poolt korraldatud töölehed ja presentatsioon RIA E-ITS (infotubestandard https://eits.ria.ee/) Andmekaitse Üldmäärus Eesti isikuandmete kaitse seadus RIA (Riigi Infosüsteemide amet) ja AKI (Andmekaitse Inspektsioon) kodulehtedel avaldatud materjalid

13. Hindamine ehk õppe lõpetamise tingimused

Hindamismeetod	Hindamiskriteerium
Testi ja kodutöö kontroll ja tagasiside	Edukaks õppe lõpetamiseks peab osaleja: - täitma kirjaliku testi, õigete vastuse % peab olema - esitama hindamisele 2 kodutööd

14. Koolitajate kvalifikatsioon

Nõutud: Soovituslik: Kõrgharidust küberturvalisuse, õigusalase või IT valdkonnas ja praktiline ametikogemus ja koolitaja kogemus viimasel 5 aastal

16. Lõpetamisel väljastatav dokument

Koolituse lõpetamisel saab iga osaleja: Tunnistust, kui õppe lõpetamise tingimused on täidetud Tõendit, kui õppe lõpetamise tingimused ei ole täidetud, kuid osaleja oli kohal