KIBERNETINIO SAUGUMO REKOMENDACIJOS DIRBANT IŠ NAMŲ

Kauno fakultetas

DARBDAVIAMS

ĮRENGINIAI, SKIRTI DARBUI
Esant galimybei, skirkite visiems darbuotojams, dirbantiems nuotoliniu būdu, tik darbui skirtus atskirus įrenginius.

NAUDOTOJO TEISĖS
Įsitikinkite, jog naudojantys darbdavio skirtus įrenginius darbuotojai juose turi tik naudotojo (t. y. neturi administratoriaus) teises.

PAGALBA
Užtikrinkite tinkamą pagalbą darbuotojams, jei kyla techninių problemų dirbant namuose.

INCIDENTŲ PRANEŠIMAS
Nustatykite tvarką, pagal kurią darbuotojai galėtų pranešti apie įtartiną įrenginio veikimą ar galimus kibernetinius incidentus, kurie kyla dirbant namuose.

ĮRENGINIŲ SAUGUMAS
Užtikrinkite, jog visi darbuotojų įrenginiai yra apsaugoti, turi gerai veikiančią, atnaujintą antivirusinę programinę įrangą su ugniasienės funkcija.

VIENINGOS TVARKOS LAIKYMASIS
Parenkite tvarką, kokiu būdu vyksta darbas nuotoliniu būdu: kur saugomi dokumentai, kam ir kokios teisės bei atsakomybės suteikiamos ir pan.

KOMUNIKACIJA
Nustatykite konkrečius saugius komunikacijos kanalus darbuotojų tarpusavio bendravimui (pvz., šifruotas el. paštas, bendravimo realiu laiku programos ir pan.)

DOKUMENTŲ BENDRINIMAS
Nustatykite priemones ar programas, kuriomis darbuotojai privalo naudotis tarpusavyje bendrindami dokumentus. Bendrinami dokumentai turėtų būti papildomai šifruojami.

KONFIDENCIALIOS INFORMACIJOS APSAUGOS UŽTIKRINIMAS
Apribokite prieigą prie visų sistemų, turinčių konfidencialią informaciją, kurios nereikalingos tuo metu darbo funkcijai atlikti.

NUOTOLINIAI SUSITIKIMAI
Organizuokite reguliarius nuotolinius susitikimus, aptarkite darbų eigą ir iškilusias problemas.

DARBUOTOJAMS

ĮRENGINIŲ NAUDOJIMAS
Nenaudokite darbui skirtų įrenginių asmeniniams tikslams. Esant galimybei, stenkitės visiškai atskirti įrenginius, naudojamus darbui ir asmeniniams poreikiams.

NUSTATYKITE SAUGIĄ PRIEIGĄ PRIE BEVIELIO WI-FI RYŠIO
Privaloma nustatyti naują Wi-Fi ir maršrutizatoriaus slaptažodį tik pradėjus dirbti namuose ir rekomenduojama šiuos slaptažodžius reguliariai, pvz., kartą kas kelis mėnesius pasikeisti. Išjunkite SSID tinklo (ang. SSID broadcast) transliaciją.

ANTROJO FAKTORIAUS AUTENTIFIKACIJA
Įsitikinkite, jog visose darbui skirtų sistemų paskyrose, kuriose įmanoma, yra įjungta antrojo faktoriaus autentifikacija.

SAUGI PROGRAMINĖ ĮRANGA
Darbui skirtuose įrenginiuose nenaudokite nelegalios programinės įrangos ir programų, kurios nesusijusios su darbine veikla. Nevenkite programų atnaujinimų ir reguliariai tai atlikite.

ĮRENGINIO APSAUGA NUO KITŲ ASMENŲ PRIEIGOS
Įrenginiams naudokite slaptažodžius ar biometrines prisijungimo priemones. Užrakinkite (ang. lock) įrenginio ekraną nors ir trumpam palikdami darbui skirtą skaitmeninį įrenginį, kad namiškiai netyčia nepadarytų žalos.

ANTIVIRUSINĖ PROGRAMINĖ ĮRANGA
Įsitikinkite, jog įrenginyje įdiegta legali antivirusinė programa, patikrinkite, kad atnaujinimai automatiškai atsiunčiami.

DOKUMENTŲ BENDRINIMAS
Dokumentų bendrinimui su kolegomis naudokite tik iš anksto darbdavio numatytą programinę įrangą. Laikykitės darbdavio nustatytų saugumo reikalavimų bendrindami dokumentus (pvz., slaptažodžiai, šifravimas ir pan.).

KOMUNIKACIJA
Bendravimui naudokite tik darbui skirtą el. pašto dėžutę ir darbdavio nurodytą realaus laiko susirašinėjimui skirtą programinę įrangą. Nenaudokite jokių asmeninių paskyrų.

SOCIALINĖ INŽINERIJA
Darbo metu nesilankykite su darbu nesusijusiose interneto svetainėse, neskubėkite spausti nuorodų el. laiškuose ir neskelbkite viešai apie darbo procese naudojamus įrankius bei metodus.

VU Kauno fakulteto
kibernetinio saugumo tyrimų grupė