Fizična

Čista miza in čist zaslon - Uporabniki so dolžni zagotoviti, da so njihove delovne površine brez vidnih občutljivih informacij ob koncu delovnega dne oziroma, ko niso prisotni na delovnem mestu.

Zaklepanje pisarn – nepooblaščenim osebam onemogočimo dostop do pisarn in občutljivih podatkov.

Nadzor nad napravami - Zaposleni so odgovorni za varovanje službenih naprav, ko so izven delovnega mesta.

Pazimo na prisluškovanje in oprezovanje, da ne prihaja do iztekanja občutljivih informacij iz podjetja.

Ne govorimo o poslovnih skrivnostih z osebami, ki za to niso pooblaščene.

Obiskovalci - Vsak obiskovalec se mora prijaviti pri receptorju/varnostniku in ga mora odgovorni zaposleni vedno spremljati. Če srečamo nepooblaščeno osebo, jo prijazno pospremimo do receptorja/varnostnika.

Najdeni dokumenti - V primeru najdbe nezaščitenih dokumentov, jih ustrezno zaščitimo oziroma predamo varnostni službi TBP.

Zaklepanje računalnikov - *Ob vsaki zapustitvi svojega delovnega mesta moramo zaposleni zakleniti računalnik. To storimo z uporabo tipke Windows + L.*

Logična

Upravljanje z gesli - Uporabljamo dovolj dolga gesla, jih NIKOLI ne posojamo ali razkrivamo.

Pri izbiri in menjavi uporabniških gesel se upoštevajo naslednja pravila:

- izbirati je potrebno gesla z najmanj 8 znakov ustrezne kompleksnosti
- znaki gesla naj vsebujejo eno malo in eno veliko črko ter vsaj eno številko
- gesla ne vsebujejo šumnikov
- gesla je potrebno menjati vsakih 12 mesecev
- vsaj 5 zaporednih gesel je neponovljivih
- geslo se zaklene za deset minut po petih nepravilnih poizkusih vnosa.

Gesla redno menjavamo

Informacij o podjetju in poslovanju ne delimo z nepooblaščenimi osebami

Dostopne pravice – se redno spremljajo in posodabljajo, vsak uporabnik ima minimalne pravice glede na delovni proces.

Oddaljen dostop do naših virov je dovoljen izključno preko poti, ki jih potrdi IT saj so samo te varne za uporabo in preverjene.

Na službene naprave nameščamo izključno preverjeno vsebino – namesti nam jo lahko samo IT služba.

Prevare in škodljiva vsebina

Ne odpiramo pošte iz sumljivih virov – e-mail naslov pošiljatelja vedno preverimo, če je ta sumljiv priponk ter povezav NE odpiramo in sporočilo označimo kot SPAM

Posredovane podatke omejimo na minimalno potrebne – Ne posredujemo podatkov, za katere menimo, da jih oseba, ki jih zahteva ne potrebuje.

V primeru dvoma o legitimnosti sporočila je potrebno to preveriti pri pošiljatelju ali IT oddelku.

Varovanje prototipov in intelektualne lastnine

Prototipi niso naša last – O njih ne govorimo in ne razkrivamo njihovih lastnosti, pri uporabi pazimo, da so ustrezno zavarovani pred zunanjimi pogledi.

Na službenih napravah je dovoljena uporaba samo licencirane programske opreme – le ta je odobrena in varna za uporabo.

Lenart, *01.03.2024*

Predstavnik vodstva za informacijsko varnost
Matjaž KOROŠEC

Direktor za kakovost in razvoj
Robert TIRŠ