**Najbolje prakse za sigurnost informacija/podataka**[[1]](#endnote-1)

Vaše poduzeće je odgovorno za zaštitu strateške tehnologije i informacija. To uključuje **“informacije u mirovanju”** (prijenosna računala, stolna računala, elektronički uređaji za pohranu, baze podataka, itd.), **“informacije u uporabi”** (SharePoint, oblak, poslužitelji datoteka i aplikacija, itd.) i **“informacije u pokretu”** (elektroničke poruke, prijenos datoteka, itd.). **U nastavku se nalazi nekoliko primjera najboljih praksi za sigurnost informacija:**

Prijenosna računala:

Izlazak iz vaše zemlje s kontroliranim tehničkim podacima ili informacijama na vašem prijenosnom računalu može predstavljati kršenje strateške kontrole trgovine u vašoj zemlji. Primjena kontrola se također može odnositi na privitke i poruke u vašim elektroničkim porukama ili datotekama na tvrdom računalnom disku.

Vaše poduzeće treba nastojati osigurati da prijenosna računala na kojima se nalaze kontrolirani podaci posjeduju odgovarajuće licence ishođene kod nacionalni tijela (ako postoje i ako su nužne) te da su podaci kodirani kako bi se spriječio neovlašteni prijenos.

**Najbolje prakse za međunarodna putovanja**

* Pripremiti detaljne smjernice i postupke za sastanke, međunarodna putovanja, elektroničke poruke, simpozije, itd. u slučaju kada će se raspravljati o kontroliranoj tehnologiji,
* Suzdržati se od slanja kontroliranih datoteka putem elektroničke pošte ili od ugrađivanja tehničkih podataka u sadržaj elektroničkih poruka. Preporuča se da vaše poduzeće datoteke dijeli samo putem poveznica na interne stranice sa sigurnom prijavom,
* Ne ostavljajte elektroničke poruke ili privitke elektroničkim porukama koji sadrže kontrolirane tehničke podatke u mapi s elektroničkom poštom. Prije odlaska na put preuzimajte informacije na sigurni poslužitelj te obrišite elektroničku poštu,
* Ne preuzimajte softver na računala s kojima će se putovati u inozemstvo,
* Osigurajte da prijenos elektroničke pošte koja sadrži kontrolirane informacije bude spremljen na sigurnom poslužitelju koji se nalazi u vašoj zemlji te da je prijenos kodiran,
* Prema potrebi, vaše bi poduzeće trebalo razmotriti mogućnost uporabe virtualne privatne mreže (VPN) za udaljeni pristup kontroliranim informacijama izvan vaše zemlje. Napomena: *Na taj način možete ukloniti potrebu da se kontrolirane informacije prenose na prijenosnom računalu zaposlenika*.

Elektronička pohrana kontroliranih informacija

Pravilna pohrana kontroliranih informacija na poslužiteljima i elektroničkim uređajima za pohranu u vašem poduzeću važan je dio u osiguravanju da se kontrolirani podaci zaštite od neovlaštenog pristupa. Nenamjerni pristup neovlaštenih osoba može predstavljati kršenje strateške kontrole trgovine u vašoj zemlji.

Kontrolirani strateški podaci se mogu osigurati pomoću kodiranja, lozinki ili pohranom na neumrežene lokacije.[[2]](#endnote-2)

**Najbolje prakse za pohranu elektroničkih podataka**

* Ograničite pohranu podataka na osobnim računalima i zajedničkim poslužiteljima,
* Vodite evidenciju o računalima, umreženim uređajima i uređajima za pohranu podataka koji održavaju kontroliranu tehnologiju; ti bi strojevi trebali biti podložni većem nadzoru sigurnosti (npr. antivirusne provjere, uključivanje vatrozida, zaključavanje sesije, kodiranje datoteke, jake lozinke). Zatražite od vašeg informatičkog odjela da na računala i uređaje postavi odgovarajuće sigurnosne zaštitne mjere,
* Opremite računala u vašem poduzeću s automatskom mogućnošću privremenog isključivanja (“time-out”) koja od korisnika traži ponovno unošenje lozinke nakon određenog vremena,
* Osigurajte da serveri s datotekama u vašem poduzeću imaju zaštitu računa/lozinki na razini mapa u katalogu podataka,
* Ograničite pristup osjetljivim mapama. Zaposlenik odgovoran za unutarnju usklađenost (ako postoji) ili glavni službenik za praćenje usklađenosti u vašem poduzeću trebaju sastaviti i čuvati ažurni popis zaposlenika ovlaštenih za pristup takvim datotekama te isti dostaviti informatičkom odjelu,
* Nemojte koristiti programe za dijeljenje datoteka (npr. Microsoft Sharepoint, Dropbox ili Box) za spremanje ili dijeljenje datoteka koje sadrže kontrolirane informacije,
* Koristite posebne uređaje za pohranu podataka (prijenosni tvrdi disk/USB memorija, itd.),
* Podatke na prijenosnim uređajima za pohranu podataka kodirajte na odgovarajući način te
* Uvedite postupke i smjernice za uništavanje/brisanje kontrolirane tehnologije kada dođe kraju svog životnog ciklusa (tvrdi diskovi, CD-ovi, DVD-ovi, USB memorije, itd.).
1. Prilagođeno i promijenjeno prema “Vodič najboljih praksi za upravljanje kontroliranim izvozom i tehnologijom u Australiji” Australian Industry Group, svibanj, 2014. [↑](#endnote-ref-1)
2. “Sveučilište u Pennsylvania, Ured za istraživanje, Obrazac plana kontrole tehnologije. [↑](#endnote-ref-2)