**Plan kontrole tehnologije (TCP)** [[1]](#endnote-1)

Ako se vaše poduzeće bavi kontroliranom tehnologijom te zapošljava strane državljane ili često održava sastanke sa stranim državljanima, preporučljivo je donijeti plan kontrole tehnologije (TCP).

Brojna poduzeća ne prepoznaju prijetnje koje predstavljaju upućene osobe ili zaposlenici koji bi potencijalno mogli zlorabiti ili prekršiti ovlašteni pristup kontroliranim informacijama/podacima kako bi ukrali osjetljivu tehnologiju ili informacije za financijsku korist ili druge zlonamjerne ciljeve (npr. krađa intelektualnog vlasništva za strana poduzeća ili vlade). Unutarnje su prijetnje doista postale uobičajena i rasprostranjena pojava u poduzećima u privatnom sektoru podjednako kao i u vladinim agencijama iz razloga koji se kreću od financijske koristi i informatičke sabotaže do ostvarivanja poslovne prednosti i industrijske špijunaže. Stoga se brojna poduzeća oslanjaju na plan kontrole tehnologije koji uvodi politike prostorne i informatičke sigurnosti te mehanizme za borbu protiv tih prijetnji.

Plan kontrole tehnologije sadrži interne postupke kojima je cilj spriječiti neovlašteni pristup kontroliranoj tehnologiji i osigurati usklađenost s nacionalnim zahtjevima strateške kontrole trgovine. Plan kontrole tehnologije trebao bi biti ugrađen u Program unutarnje usklađenosti (ICP) poduzeća i sadržavati dodatne karakteristike **plana prostorne sigurnosti, plana informacijske sigurnosti i postupke za provjeru zaposlenika**.

**Elementi plana kontrole tehnologije**

**Sveobuhvatan plan kontrole tehnologije bi trebao uključivati sljedeće korake kako bi pridonio osiguranju pravilnog upravljanja strateškom tehnologijom i informacijama:**

* Donijeti sveobuhvatnu politiku poduzeća u kojoj su identificirani relevantni propisi i zakoni te koji obvezuje na usklađenost sa zahtjevima strateške kontrole trgovine;
* Popisati domaće i strane zahtjeve strateške kontrole trgovine vezane za prijenos tehnologije;
* Jasno definirati što se smatra „kontroliranom tehnologijom” i definirati ostalu relevantnu tehnologiju;
* Odrediti ovlaštenog zaposlenika/zaposlenike za usklađenost koji će biti zadužen/i za upravljanje i nadzor plana kontrole tehnologije, uključujući podatke za kontakt;
* Definirati uloge i odgovornosti zaposlenika zaduženog za upravljanje planom kontrole tehnologije (npr. referent za kontrolu tehnologije);
* Uskladiti zahtjeve, postupke i postupke za kontrolu tehnologije;
* Odrediti zaposlenike poduzeća na koje se zahtjevi primjenjuju;
* Specificirati odgovornosti zaposlenika te obveze izvođača i dobavljača;
* Utvrditi lokaciju kontroliranih „tehničkih podataka” te objekte i prostorije gdje se primjenjuju ograničenja;
* Pripremiti smjernice vezane za **informatičku sigurnost i pristup informatičkim sustavima** kako bi se spriječio neovlašteni prijenos kontrolirane tehnologije:
* Zaštita lozinkom, prijava, zaključavanje sesije
* Enkripcija datoteka, korištenje vatrozida
* Antivirusne provjere i provjere kibernetičke sigurnosti
* Korištenje virtualnih privatnih mreža (VPN) i neumreženih servera
* Uništavanje/brisanje kontrolirane tehnologije
* Uvesti **mjere prostorne sigurnosti** kako bi se spriječio neovlašteni pristup. Potrebno je opisati prakse vezane za:
* Kontrolu pristupa
* Identifikaciju i kontrolu posjetitelja
* Pohranu dokumenata i podataka
* Zbrinjavanje kontroliranih informacija
* Svi postupci uvoza i izvoza, uključujući nematerijalne prijenose, trebaju sadržavati postupke za reviziju i dokumentiranje kako bi se spriječio neovlašteni prijenos u svakoj ključnoj fazi;
* Opisati i uspostaviti sustav klasificiranja kako bi se kontrolirane informacije jasno razlikovale i klasificirale. Sustav bi trebao kontroliranu tehnologiju zaštititi od nekontrolirane tehnologije;
* Na odgovarajući način opisati postupke za kontrolu, pohranu, rukovanje i zbrinjavanje dokumenata;
* Uvesti postupke za provjeru zaposlenika kako bi se osiguralo da nemaju kriminalnu prošlost ili da nisu povezani s označenim subjektima ili pojedincima koji su uključeni u aktivnosti širenja oružja. Napomena: *Kod provjere zaposlenika na različitim popisima označenih subjekata možete upotrijebiti alat za provjeru strana s ograničenim pravima koji je dio Vodiča za program unutarnje usklađenosti.*

Napomena: *Dodatak 1. ovom dijelu sadrži „Obrazac programa kontrole tehnologije” koji vaše poduzeće može prilagoditi i koristiti. Nadalje, ovaj dio sadrži informacije pomoću kojih vaše poduzeće može donijeti „Plan kontrole pristupa stranih državljana”.*

1. Prilagođeno i izmijenjeno iz: „Australian Best Practice Guide for the Management of Controlled Exports and Technologyˮ (Australski vodič za najbolje prakse u vezi upravljanja kontroliranim izvozom i tehnologijom), Australian Industry Group, svibanj 2014., < http://pdf.aigroup.asn.au/13266\_ecf\_best\_practice\_guide\_cover\_web.pdf>. [↑](#endnote-ref-1)