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

Ukoliko vaše preduzeće posluje sa kontrolisanim tehnologijama, zapošljava strane državljane ili organizuje redovne sastanke sa stranim državaljanima, preporuka je da vaše preduzeće izradi Plan za kontrolu tehnologije (TCP).

Veliki broj preduzeća ne prepoznaje pretnje koje podrazumeva prisustvo lica ili zaposlenih koji potencijalno mogu da zloupotrebe ili prekorače nivo dozvoljenog pristupa kontrolisanim informacijama/ podacima i nezakonito prisvoje osetljive tehnologije ili informacije zarad finansijske dobiti ili drugih malicioznih ciljeva (na primer, krađa intelektualne svojine za inostrana preduzeća ili vlade). I zaista, pretnje unutar samog preduzeća postale su uobičajena i popularna pojava koja na meti ima ne samo preduzeća u privatnom sektoru, već i državne agencije, zarad ostvarivanja različitih ciljeva koji se kreću od finansijske dobiti, preko sabotaže u IT domenu, do sticanja poslovne prednosti i industrijske špijunaže. Kao rezultat toge, većina preduzeća se odlučuje da se u tom pogledu osloni na planove za kontrolu tehnologije kojima se uspostavljaju politike i mehanizmi fizičke i IT bezbednosti za borbu protiv pomenutih pretnji.

Plan za kontrolu tehnologije (TCP) uspostavlja interne procedure koje za cilj imaju sprečavanje neovlašćenog pristupa kontrolisanoj tehnologiji i obezbeđivanje poštovanja zahteva i propisa koji se odnose na kontrolu spoljne trgovine strateškom robom. Plan za kontrolu tehnologije treba da predstavlja sastavni deo Programa interne usklađenosti preduzeća i da sadrži dodatne funkcije kao što su **plan fizičke bezbednosti, plan informatičke bezbednosti i procedure za proveru zaposlenih.**

**Elementi Plana za kontrolu tehnologije (TCP)**

**Da bi obezbedio pravilno upravljanje tehnologijom i informacijama od strateškog značaja, sveobuhvatni plan za kontrolu tehnologije treba da sadrži sledeće:**

* Sveobuhvatnu izjavu o poslovnoj politici koja identifikuje relevantne propise i zakone i nalaže usklađenost sa propisima o kontroli spoljne trgovine strateškom robom;
* Dokumentovane domaće i inostrane zahteve u oblasti kontrole spoljne trgovine strateškom robom koji se odnose na transfer tehnologija;
* Jasno definisane „kontrolisane tehnologije“ i definicije drugih relevantnih pojmova;
* Određeno jedno ili više ovlašćenih lica za usklađenost i odgovornih za upravljanje i nadgledanje realizacije Plana za kontrolu tehnologije, sa odgovarajućim kontakt podacima;
* Definisane uloge i odgovornosti lica odgovornih za upravljanje Planom za kontrolu tehnologije (na primer, glavni službenik za usklađenost);
* Formulisane zahteve, procese i procedure za kontrolu tehnologije;
* Prepoznati lica u preduzeću na koja se zahtevi odnose;
* Odgovornosti zaposlenih i obaveze izvođača i dobavljača;
* Tačne lokacije kontrolisanih „tehničkih podataka“ i objekte na koje se primenjuju ograničenja;
* Smernice koje se odnose na **informatičku bezbednost i pristup IT sistemima** u cilju sprečavanja neovlašćenog transfera kontrolisane tehnologije:
* zaštita lozinkom, prijava, zaključavanje sesije,
* šifriranje datoteka, firewall,
* antivirusne i provere sajber bezbednosti,
* upotrebna Virtualnih privatnih mreža odnosno *Virtual Private Networks* (VPNs) i servera koji nisu na mreži,
* uništavanje/ brisanje kontrolisanih tehnologija.
* Uspostavljene **mere fizičkog obezbeđenja** radi sprečavanja neovlašćenog pristupa. Treba opisati prakse koje se odnose na:
* kontrolu pristupa,
* legitimisanje i kontrolu posetilaca,
* skladištenje dokumenata i podataka,
* odlaganje kontrolisanih informacija,
* Svi procesi kod uvoza i izvoza, uključujući nevidljive transfere, treba da obuhvataju procedure za pregled i dokumentovanje u svim ključnim fazama, u cilju sprečavanja neovlašćenog transfera,
* Sistem klasifikacije treba da bude uspostavljen i opisan kako bi na odgovarajući način razlikovao i klasifikovao sve kontrolisane informacije. Sistem takođe treba da nastoji da odvoji (firewall) kontrolisanu tehnologiju od one koja ne podleže kontroli;
* Podrobno opisane postupke za kontrolu, skladištenje, rukovanje i odlaganje dokumenta;
* Razviti procedure za proveru zaposlenih kako bi se osiguralo da se ne nalaze u kaznenoj evidenciji ili da nemaju veze sa određenim privrednim subjektima ili pojedincima koji su učestvovali u aktivnostima širenja naoružanja. Napomena: *Alat za kontrolu lica na koja se primenjuju ograničenja koji predstavlja sastavni deo Vodiča za Program interne usklađenosti može da posluži kao način za proveru zaposlenih u odnosu na različite utvrđene liste lica.*

Napomena: *Prilog 1 ovog odeljka sadrži primer Plana za kontrolu tehnologije koji vaše preduzeće može da prilagodi sopstvenim potrebama. Dalje, odeljak nudi informacije koje vašem preduzeću omogućavaju definisanje Plana za kontrolu pristupa stranih državljana.*

1. Prilagođeno i modifikovano iz “Australian Best Practice Guide for the Management of Controlled Exports and Technology,” Australian Industry Group, May 2014, < http://pdf.aigroup.asn.au/13266\_ecf\_best\_practice\_guide\_cover\_web.pdf>. [↑](#endnote-ref-1)