**Dobre prakse u pogledu fizičke bezbednosti**

* **Jasno prepoznati kontrolisane tehnologije** **→** Kontrolisana roba mora biti jasno označena kao „kontrolisana“ i fizički odvojena zbog razlikovanja od tehnologija i informacija koje ne podležu kontroli. Jedan od načina za fizičko razdvajanje može biti klasifikacija, odnosno svrstavanje informacija u odgovarajuće kategorije, kao na primer: 1) za javnu upotrebu, 2) samo za internu upotrebu 3) poverljivi/ kontrolisani podaci.
* Zatim, vaše preduzeće treba da „označi“, odnosno na odgovarajući način klasifikuje tehnologije ili informacije koje smatra osetljivim ili koje podležu kontroli. Robni klasifikacioni broj (CCN) dodeljuje se svim podacima od strateškog značaja koji se nalaze na nacionalnoj kontrolnoj listi, i te informacije treba katalogizovati u bazama podataka/ datotekama za buduću upotrebu.
* **Napraviti sigurno fizičko skladište →** Kontrolisana tehnologija, kada nije u upotrebi ili posedu ovlašćenih lica preduzeća, treba da bude pod ključem u obezbeđenom prostoru (ormanu, sefu, fioci).
* Koristite princip „jedne brave“. Princip „jedne brave“ za obezbeđivanje kontrolisane robe i sprečavanje njenog otkrivanja neovlašćenim licima zahteva korišćenje barem jednog sigurnosnog mehanizma (ključeva, kartica, pristupnih šifara, itd.). Napomena: *Ovo predstavlja minimum zahteva neophodan za zaštitu i obezbeđivanje kontrolisanih tehnologija i informacija.*[[1]](#endnote-1)
* Datoteke, odnosno dokumenta u papirnoj verziji koja sadrže kontrolisane informacije ili tehnologiju treba čuvati pod ključem (npr. u obezbeđenom i zaključanom ormanu u kancelariji koja se, kada se ne koristi, zaključava).[[2]](#endnote-2)
* Kontrolisana tehnologija koja ne može da se čuva u obezbeđenom prostoru/ kontejneru kada se ne koristi može zahtevati dodatne mere obezbeđenja. Ovaj vid „otvorenog“ skladištenja po pravilu je manje bezbedan i nosi veći rizik od nehotičnog transfera kontrolisane tehnologije i informacija.[[3]](#endnote-3)
* Preporuka je da se kontrolisane informacije ne iznose iz obezbeđenog mesta u kojem se čuvaju bez odobrenja odgovarajućeg ovlašćenog službenika vašeg preduzeća zaduženog za usklađenost poslovanja.
* Potrebno je uspostaviti procedure za pravilno uništavanje i odlaganje kontrolisanih informacija (npr. papira, shema, nacrta).
* **Uspostaviti područja sa ograničenim pristupom** **→** Područja sa ograničenim pristupom koriste se za regulisanje pristupa kontrolisanim tehnologijama koje se tokom radnog vremena nalaze na otvorenom. Radni prostori sa ograničenim pristupom često imaju fizičke barijere koje kontrolisane informacije štite od usmenog ili vizuelnog transfera neovlašćenim licima.
* Zone ograničenog pristupa treba da imaju jasno definisane granice, dok fizičke barijere nisu uvek neophodne.
* Zone ograničenog pristupa predstavljaju pametno rešenje u situacijama u kojima nije praktično, a ni moguće da se u određenim oblastima, zbog formata, veličine, obima ili drugih neobičnih karakteristika, kontrolisane tehnologije zaštite od neovlašćenog pristupa.
* Lica unutar zona sa ograničenim pristupom odgovorna su za onemogućavanje ulaska licima koja nemaju odgovarajuća ovlašćenja.
* **Uvesti kontrole pristupa →** Veliki broj preduzeća pribegava metodama za kontrolu pristupa kako bi se osiguralo da pristup kontrolisanoj tehnologiji imaju samo ovlašćena lica.
* Upotrebite ključne kontrole za upravljanje pristupom kontrolisanoj tehnologiji. Ključne kontrole mogu biti manuelne, mada je bolje da budu elektronske prirode (na primer, kartice ili tasteri sa šiframa za svakog pojedinačnog zaposlenog).
* Uspostavite stalan video nadzor i CCTV praćenje pristupa kontrolisanim tehnologijama.
* Uspostavite politiku pojedinačnog ulaska, pri čemu svaki zaposleni pojedinačno pristupa zonama sa ograničenim pristupom ili zonama sa kontrolisanim tehnologijama pomoću svog ključa, kartice, pristupne šifre ili akreditiva (nastojte da zabranite istovremeni ulazak dvoje ljudi).
* Uspostavite postupak prijave za dobijanje dozvole za pristup kontrolisanoj tehnologiji ili opremi. Kontrolisane informacije, kada je moguće, treba čuvati u zaključanim prostorima za koje je utvrđen postupak odjave, čime se omogućava vođenje dnevnika pristupa. U slučaju da to nije moguće, preduzeće bi trebalo da razmotri upotrebu zona sa ograničenim pristupom čime se omogućava vođenje evidencije lica koja ulaze i izlaze iz tih zona.[[4]](#endnote-4)
* Napravite dnevnik pristupa koji sadrži detalje o svim pojedincima koji su boravili u zonama sa ograničenim pristupom ili zonama sa kontrolisanim tehnologijama.
* **Razviti mere za legitimisanje i kontrolu posetilaca** **→** Vaše preduzeće dužno je da obezbedi da se posetiocima ne omogući pristup (vizuelno ili usmeno) kontrolisanoj tehnologiji, osim u slučajevima kada za pristup postoji odgovarajuća dozvola koju su izdali državni organi. **Vaše preduzeće može da preduzme sledeće mere da se spreči da posetioci imaju pristup kontrolisanoj tehnologiji i informacijama, i zadrži usklađenost sa propisima o kontroli spoljne trgovine strateškom robom:**
* *Provera* → Preporuka je da vaše preduzeće unapred proveri posetioce i uveri se da se ne nalaze na listi fizičkih i pravnih lica na koja se primenjuju ograničenja (Napomena: *Vaše preduzeće za proveru posetilaca u odnosu na relevantne liste može da upotrebi Alat za proveru lica na koja se primenjuju ograničenja (RPST)*). Pored toga, važna informacija može biti i unapred utvrđeno državljanstvo posetioca, **jer pojedine države imaju utvrđena ograničenja na transfere kontrolisane tehnologije određenim stranim državljanima**. Vaše preduzeće može da razmotri i uvođenje pregleda viza/ radnih biografija stranih državljana kako bi se uverilo da posetilac ne predstavlja nepotreban rizik, odnosno da nije povezan sa određenim licima, zainteresovanim stranama ili odredištima.
* *Registar posetilaca* → Preporuka je da vaše preduzeće od svih posetilaca zahteva da se na ulazu u objekte preduzeća upišu, odnosno registruju. Vaše preduzeće dužno je da utvrdi da li je posetilac ovlašćen da pristupi kontrolisanim informacijama, i da obezbedi odgovarajuću karticu i/ili pratnju.
* *Pratnja za posetioce i identifikacione značke tj. kartice* → Svi posetioci dužni su da nose dobijene identifikacione kartice. Identifikaciona kartica posetioca treba da bude lako prepoznatljiva i vidljiva u svakom trenutku boravka u objektima preduzeća. Posetioci koji nemaju pristup kontrolisanim informacijama treba da u svakom trenutku budu pod pratnjom zaposlenih i da nose odgovarajuće identifikacione kartice, odnosno značke za posetioce.[[5]](#endnote-5) Pojedina preduzeća omogućavaju značke sa RFID tagovima (identifikacija putem radio frekvencije) za kontrolisanje fizičke udaljenosti između posetilaca i kontrolisane tehnologije.
* *Ugovori o čuvanju poverljivih podataka* → Vaše preduzeće može da razmotri uvođenje obaveze posetilaca o priznavanju postojanja Programa interne usklađenosti (i/ili Plana za kontrolu tehnologije) i da od posetilaca zahteva potpisivanje sporazuma o čuvanju podataka, koji ih obavezuje na neobjavljivanje informacija u vezi sa posetom. Napomena: *Prilog 2 ovog odeljka sadrži Model sporazuma o poverljivosti podataka koji podležu kontroli, koji vaše preduzeće može da prilagodi sopstvenim potrebama.*
* *Fizički pregled* → Vaše preduzeće može da razmotri fizički pregled torbi, paketa i elektronskih medija za čuvanje podataka pri ulasku u objekat. Posetioci mogu da budu zamoljeni da svoje mobilne telefone i druge elektronske uređaje ostave na ulazu u objekat sa kontrolisanim tehnologijama od strateškog značaja.
* *Kontrola pristupa trećim licima* → Vaše preduzeće može da razmotri i uvođenje kontrole koja domare, radnike na održavanju i upravljanju zgradom sprečava od neovlašćenog pristupa kontrolisanim informacijama.[[6]](#endnote-6)
1. Beran, Mary and David Brady, "Using Technology Control Plans in Export Compliance," University of Pennsylvania, 2013, <http://www.upenn.edu/researchservices/Export%20Controls%20Conference/Mary%20Beran%20&%20David%20Brady%20-%20Using%20Technology%20Control%20Plans%20in%20Export%20Compliance.pdf>.

2 “University of Pennsylvania Office of Research Services TCP Template,” University of Pennsylvania, available at, <http://www.upenn.edu/researchservices/exportcontrols/documents/annotated%20TCP%20Template%20v3.docx>.

3 Beran, Mary and David Brady, "Using Technology Control Plans in Export Compliance," University of Pennsylvania, 2013.

4 “University of Pennsylvania Office of Research Services TCP Template,” University of Pennsylvania.

5 “Australian Best Practice Guide for the Management of Controlled Exports and Technology,” Australian Industry Group, May 2014.

6 Beran, Mary and David Brady, "Using Technology Control Plans in Export Compliance," University of Pennsylvania, 2013. [↑](#endnote-ref-1)
2. [↑](#endnote-ref-2)
3. [↑](#endnote-ref-3)
4. [↑](#endnote-ref-4)
5. [↑](#endnote-ref-5)
6. [↑](#endnote-ref-6)