**Najbolje prakse prostorne sigurnosti**

* **Jasno identificirajte kontroliranu tehnologiju** **→** Sva kontrolirana roba mora imati jasnu oznaku „kontrolirano” te se mora jasno razlikovati i biti prostorno odvojena od nekontrolirane tehnologije i informacija. Informacije se mogu klasificirati prema sljedećim kategorijima podataka: 1) javna uporaba, 2) samo za internu uporabu i 3) povjerljivo/kontrolirano.
* Nadalje, u vašem se poduzeću svaka tehnologija ili informacija koja se smatra osjetljivom ili podložnom kontroli može označiti ili klasificirati na odgovarajući način. Svakom strateškom podatku koji se nalazi na nacionalnoj kontrolnoj listi treba dodijeliti klasifikacijski broj robe (CCN), a te informacije treba katalogizirati u baze podataka/datoteke za buduću uporabu.
* **Napravite sigurno prostorno skladište →** Kontrolirana tehnologija treba biti zaključana u sigurnom spremniku (ormarić, sef, ladica) kada nije u posjedu ili kada je ne koriste ovlašteni zaposlenici poduzeća.
* Koristite „načelo jedne brave”. Načelo „jedne brave” za zaštitu kontrolirane robe zahtijeva korištenje barem jednog mehanizma (ključa, kartice-ključa, pristupnog koda i sl.) za sprječavanje razotkrivanja podataka neovlaštenim osobama. Napomena: *Ovo je minimalni zahtjev za zaštitu kontrolirane tehnologije i informacija*.[[1]](#endnote-1)
* Dokumentacija u tiskanom obliku koja sadrži kontrolirane informacije ili tehnologiju treba biti pohranjena pod ključem (npr. u sigurnom, zaključanom ormariću za spise u uredu koji je zaključan kada u njemu nema nikoga).[[2]](#endnote-2)
* U slučaju kontrolirane tehnologije koja se ne može pohraniti u sigurni spremnik kada se ne koristi možda će biti potrebne dodatne sigurnosne mjere. Ova vrsta „otvorene” pohrane najčešće je manje sigurna i predstavlja veći rizik od nenamjernog prijenosa kontrolirane tehnologije i informacija.[[3]](#endnote-3)
* Preporuča se da se kontrolirane informacije ne uklanja iz skladišta bez odobrenja osobe ovlaštene za usklađenost u vašem poduzeću.
* Uvedite postupke za pravilno uništavanje i odlaganje kontroliranih informacija (npr. papira, grafičkih prikaza, nacrta).
* **Odredite ograničena područja** **→** Ograničena područja se koriste za regulaciju pristupa kontroliranoj tehnologiji koja je tijekom radnog vremena smještena u otvorenom području. U ograničenim radnim područjima se često koriste fizičke prepreke za zaštitu od usmenog ili vizualnog prijenosa kontroliranih informacija neovlaštenim pojedincima.
* Ograničeno područje treba imati jasno određene parametre, no fizičke prepreke nisu uvijek potrebne.
* Ograničeno područje je korisno kada je nepraktično ili nemoguće zaštititi pristup kontroliranoj tehnologiji zbog njenog oblika, veličine, količine ili neke druge neobične karakteristike.
* Zaposlenici unutar ograničenog područja su odgovorni za kontrolu svih zaposlenika koji nemaju odgovarajuće ovlaštenje za ulazak u ograničeno područje.
* **Uvedite kontrolu pristupa →** Brojna poduzeća koriste kontrolu pristupa kako bi osigurala da kontrolirana tehnologija bude dostupna samo ovlaštenom osoblju.
* Koristite kontrolu ključem za upravljanje pristupom kontroliranoj tehnologiji. Kontrola ključem može biti manualna, ali je bolje da bude elektronička (npr. kartica-ključ ili kontrolne tipkovnice s pristupnim kodovima za svakog zaposlenika).
* Neprekidno koristite video nadzor i nadzorne kamere kako biste nadzirali pristup kontroliranoj tehnologiji.
* Uvedite politiku pojedinačnog ulaska pri čemu svaki zaposlenik mora zasebno ulaziti u ograničeno područje ili pristupati kontroliranoj tehnologiji koristeći svoj ključ, značku, pristupni kod ili akreditaciju (nastojte zabraniti da dvije osobe ulaze istovremeno).
* Zahtijevajte registraciju za pristup kontroliranoj tehnologiji ili opremi. Kada je moguće, kontrolirane informacije treba pohraniti u zaključane spremnike s uspostavljenim postupcima za odjavu tako da se može pratiti sljedivosti. Ako to nije moguće, poduzeće treba razmisliti o korištenju ograničenih područja da bi se moglo pratiti tko je ušao i izašao.[[4]](#endnote-4)
* Vodite evidenciju pristupa s detaljnim podacima o pojedincima koji su ušli u ograničeno područje ili koji su pristupili kontroliranim informacijama ili tehnologiji.
* **Uspostavite mjere identifikacije i kontrole posjetitelja**  **→** Vaše poduzeće je dužno osigurati da posjetitelji nemaju (vizualni ili usmeni) pristup kontroliranoj tehnologiji, osim u slučaju da imaju dozvolu nadležnog nacionalnog tijela. **Vaše poduzeće može poduzeti sljedeće korake da bi se posjetiteljima spriječio pristup kontroliranoj tehnologiji i informacijama te zadržala usklađenost sa zahtjevima strateške kontrole trgovine:**
* *Provjera*  → Preporučuje se da se u vašem poduzeću prethodno izvrše provjere posjetitelja da bi se na taj način osiguralo da se oni ne nalaze na popisu strana ili subjekata s ograničenim pravima (Napomena: *Vaše poduzeće može upotrijebiti alat za provjeru strana s ograničenim pristupom (RPTS) i tako provjeriti nalaze li se posjetitelji na relevantnim popisima*). Nadalje, možda je važno unaprijed utvrditi državljanstvo posjetitelja budući da **neke države imaju ograničenja u vezi prijenosa kontrolirane tehnologije određenim stranim državljanima**. Vaše bi poduzeće također moglo razmotriti mogućnost o provjere životopisa/vize kako bi se osiguralo da posjetitelji ne predstavljaju nepotreban rizik ili da nemaju veze s određenim stranama, pojedincima ili odredištima.
* *Registar posjetitelja* → Preporuča se da se svi posjetitelji potpišu u registar posjetitelja prije ulaska u prostorije vašeg poduzeća. Vaše je poduzeće dužno utvrditi ima li posjetitelj pravo na pristup kontroliranim informacijama te osigurati odgovarajuću oznaku i/ili pratnju.
* *Pratnja za posjetitelja i identifikacijske oznake* → Svi posjetitelji moraju nositi identifikacijske oznake. Identifikacijske oznake posjetitelja moraju biti lako prepoznatljive i vidljivo izložene tijekom cijelog boravka u prostorijama vašeg poduzeća. Posjetitelji koji nemaju pravo pristupa kontroliranim informacijama trebaju uvijek biti u pratnji zaposlenika i moraju stalno nositi identifikacijske kartice/oznake.[[5]](#endnote-5) Neka poduzeća koriste oznake s radiofrekvencijskom identifikacijom (RFID) za praćenje prostorne udaljenosti posjetitelja od kontrolirane tehnologije.
* *Ugovor o povjerljivosti* → Vaše bi poduzeće moglo zahtijevati da posjetitelji potvrde svoje saznanje o programu unutarnje usklađenosti (ICP) (i/ili planu kontrole tehnologije) te da potpišu ugovor o povjerljivosti sukladno kojemu posjetitelji ne smiju odavati bilo kakve informacije vezane uz posjet. Napomena: *Dodatak 2. ovom dijelu sadrži „Obrazac ugovora o povjerljivosti kontroliranih informacija” koji se može prilagoditi potrebama vašeg poduzeća.*
* *Fizičke provjere* → Vaše bi poduzeće pri ulasku moglo provoditi fizičku provjeru torbi, paketa i medija za elektroničku pohranu. Posjetitelji bi morali ostaviti mobilne telefone ili ostale elektroničke uređaje prije ulaska u prostorije u kojima se nalazi kontrolirana strateška tehnologija.
* *Kontrola pristupa trećih strana* → Vaše bi poduzeće moglo uvesti kontrole koje bi čuvarima i osoblju za održavanje i upravljanje zgradom ograničile pristup kontroliranim informacijama.[[6]](#endnote-6)
1. Beran, Mary i David Brady, „Using Technology Control Plans in Export Complianceˮ, Sveučilište u Pennsylvaniji, 2013., <http://www.upenn.edu/researchservices/Export%20Controls%20Conference/Mary%20Beran%20&%20David%20Brady%20-%20Using%20Technology%20Control%20Plans%20in%20Export%20Compliance.pdf>. [↑](#endnote-ref-1)
2. “Sveučilište u Pennsylvaniji, Ured za usluge istraživanja, Obrazac plana kontrole trgovine”, Sveučilište u Pennsylvaniji, dostupno na: <http://www.upenn.edu/researchservices/exportcontrols/documents/annotated%20TCP%20Template%20v3.docx>. [↑](#endnote-ref-2)
3. Beran, Mary i David Brady, „Using Technology Control Plans in Export Complianceˮ, Sveučilište u Pennsylvaniji, 2013. [↑](#endnote-ref-3)
4. “Sveučilište u Pennsylvaniji, Ured za usluge istraživanja, Obrazac plana kontrole trgovine ”, Sveučilište u Pennsylvaniji. [↑](#endnote-ref-4)
5. „Australian Best Practice Guide for the Management of Controlled Exports and Technologyˮ, Australian Industry Group, svibanj 2014. [↑](#endnote-ref-5)
6. Beran, Mary i David Brady, „Using Technology Control Plans in Export Complianceˮ, Sveučilište u Pennsylvaniji, 2013. [↑](#endnote-ref-6)