**Prilog 4: Model obrasca za podatke o kontroli pristupa**[[1]](#endnote-1)

**[Uneti naziv preduzeća]**

**Datum:**

**Opis robe (i robni klasifikacioni broj (CCN)):**

**Odgovorno lice/ pozicija:**

**Lokacija:** \_\_\_\_\_\_\_\_\_soba br., \_\_\_\_\_\_\_\_\_ zgrada br., [uneti punu adresu].

**Organizacija (odeljenje, program ili projekat):**

**Opis, relevantne tehničke specifikacije i performanse robe (na primer,** digitalni računari sa 2688 Intel Itanium procesorima i 384 MIPS procesorima sa računarskim mogućnostima koje prelaze 190 miliona MTOPS)

**Kontrole spoljne trgovine strateškom robom i ograničenja:** (navedite odgovarajuće zakonske odredbe ili ograničenja koja se odnose na krajnje namene odnosno krajnje korisnike)

Ovlašćeni pristup**:**

**Fizička lokacija i oblasti tj. zone sa ograničenim pristupom:**

1. Pristup bez pratnje \_\_\_\_\_\_\_sobi ili \_\_\_\_\_\_prostorijama dozvoljen je samo ovlašćenim licima.
2. Samo ovlašćenim licima dozvoljen je pristup radnim oblastima sa ograničenim pristupom, a koje sadrže kontrolisane tehnologije.
3. Pre obilaska, [uneti poziciju odgovornog lica] vrši proveru prostorije da bi se obezbedilo da kontrolisane tehnologije nisu vidljive.
4. Svi zaposleni koji su u poseti prostorijama [uneti naziv vašeg preduzeća] moraju biti pod stalnom pratnjom.
5. [uneti dodatne informacije].

**Fizička bezbednost:**

1. Postoji [uneti tačan broj ulaza] ulaza u \_\_\_\_\_\_\_\_\_\_prostoriju. Ukupno [uneti broj ulaza] ulaza se kontroliše pomoću [RFID znački] i obezbeđeno je [bravama, pristupnim šiframa ili kontrolnim panelima].
2. Sve ulazne tačke su pod video nadzorom i permanentno se prate preko CCTV sistema.
3. Ovlašćeni [uneti poziciju ovlašćenog službenika za usklađenost] odobrava pristup \_\_\_\_\_\_\_\_ prostoriji.
4. Prostorija \_\_\_\_\_\_\_\_\_ nalazi se pod nadzorom nadležnog osoblja 24 sata dnevno, 7 dana u nedelji.
5. [uneti dodatne informacije].

**IT bezbednost:**

1. Daljinski pristup serverima na kojima se nalaze kontrolisani tehnički podaci dozvoljen je samo ovlašćenim nalozima. Postoje dve grupe naloga: **administratori** – sa privilegovanim pristupom, i **korisnici** – sa neprivilegovanim, odnosno ograničenim pristupom.
2. ,,Ovlašćeni nalozi” su nalozi koji zadovoljavaju određene zahteve koje utvrđuje administrator sistema. Svi nalozi se rutinski proveravaju radi utvrđivanja odgovarajućeg nivoa dozvoljenog pristupa.
3. Svi nivoi pristupa zahtevaju odgovarajuću autentifikaciju, dok se sve lozinke čuvaju u skladu sa zahtevima politike preduzeća koji se odnose na lozinke.
4. [uneti dodatne informacije].

**Informisanost:**

1. Svi zaposleni i posetioci koji su strani državljani obavešteni su o ograničenjima u okviru kontrole spoljne trgovine strateškom robom koja se odnose na datu robu, kao i o granicama pristupa kontrolisanim tehnologijama i informacijama bez dozvole nadležnih državnih organa.
2. [uneti dodatne informacije].

**Prijavljivanje povreda propisa:**

Pojedinci koji veruju da je došlo do povrede propisa o kontroli spoljne trgovine strateškom robom, bilo da je reč o namernoj ili slučajnoj povredi propisa, svoje bojazni prijavljuju [uneti naziv supervizora odeljenja/ administratora ili ovlašćenog službenika za usklađenost], koji će o tome obavestiti glavnog službenika/ direktora za usklađenost (CCO).

1. Prilagođeno i modifikovano iz “Guidance for creating access control plans,” U.S. National Oceanic and Atmospheric Administration (NOAA), 2014, <http://deemedexports.noaa.gov/access\_control\_plans/access-control-plan-guidance.pdf>. [↑](#endnote-ref-1)