D-13442/1

CRNA GORA

MINISTARSTVO FINANSIJA

UPRAVA CARINA

POLITIKA INFORMACIONE BEZBJEDNOSTI

SADRŽAJ

ZAPIS O DOPUNI (VERZIJI DOKUMENTA)

a.	*Verzija:*	
b.	*Datum:*	
c.	*Izmjena na strani:*	
d.	*Opis izmjene:*	
e.	*Podnosilac zahtjeva za izmjenu:*	

SKRAĆENICE

MF	Ministarstvo finansija
MJU	Ministarstvo javne uprave
UC	Uprava carina
IS	Informacioni sistem
IB	Informaciona bezbjednost
CIS	Carinski informacioni sistem
PIB	Politika informacione bezbjednosti
SIB	Savjetnik za informacionu bezbjednost

POJMOVI

- ***Informacioni sistem*** (IS) je integrisani skup komponenti za sakupljanje, snimanje, čuvanje, obradu i prenošenje podataka.
- ***Informaciona bezbjednost*** (IB) podrazumijeva stanje povjerljivosti, cjelovitosti i dostupnosti podataka.
- ***Podatak*** je informacija, poruka i dokument sačinjen, poslat, primljen, zabilježen, skladišten ili prikazan elektronskim, optičkim ili sličnim sredstvom, uključujući prenos internetom i elektronsku poštu.
- ***Povjerljivost podatka*** podrazumijeva da je podatak dostupan samo licima koja su ovlašćena da ostvare pristup ili postupe sa tim podatkom.
- ***Cjelovitost*** podatka podrazumijeva očuvanje postojanja, tačnosti i kompletnosti podatka, kao i zaštitu procesa ili programa koji sprječavaju neovlašćeno mijenjanje podatka.
- ***Dostupnost podatka*** podrazumijeva da ovlašćeni korisnici mogu da pristupe podatku uvijek kada za tim imaju potrebu.
- ***Resursi informacionog sistema*** *uključuju*
  - **Hardverska imovina** – računari i računarska oprema, komunikaciona oprema, sistemi za skladištenje podataka kao i ostala tehnička oprema koja podržava rad informacionog sistema
  - **Softverska imovina** – operativni sistemi, programi za nadzor informacionog sistema, sigurnosni programi, korisnički programi, programi za upravljenje bazama podataka, alati za razvoj programa, uslužni programi i ostali programi koji se nalaze na informacionim sistemima.
  - **Informaciona imovina** – podaci u bazama podataka, dokumenta sa podacima, programski kod u tekstualnom obliku, dokumentacija o informacionim sistemima i programima, priručnici, planovi i usluge informacionog sistema.
- ***Grupa za bezbjednost i standardizaciju (02/01-1)*** – Pravilnik o unutrašnjoj organizaciji i sistematizaciji Uprave carina. Grupa je formirana u okviru Sektora za carinsko-informacioni sistem (02), Odsjek za sistemsku podršku i razvoj (02/01).
- ***Savjetnik za informacionu bezbjednost (SIB)*** *– carinski službenik koji pokriva poziciju "Samostalni/a carinski/a savjetnik/ca I – specijalista za IT bezbjednost"* u Grupi za bezbjednost i standardizaciju.

1. SVRHA

Politika informacione bezbjednosti (PIB) Uprave carina predstavlja krovni dokument u kome se definišu vodeća načela i odgovornosti potrebne za zaštitu informacionog sistema ove institucije.

Svrha PIB-a je obezbjeđivanje bezbjednosnih okvira koji će osigurati zaštitu podataka UC od neovlašćenog pristupa, gubitka i oštećenja, zloupotrebe, dok podržava potrebe za sigurnom razmjenom informacija.

Druge politike, procedure i priručnici koje se odnose na PIB pružaju dodatne detalje za njeno sprovođenje. Sva dodatna dokumenta su razvijena i objavljena odvojeno.

2. PODRUČJE PRIMJENE

PIB se odnosi na sve zaposlene u UC i na ostale pojedince i subjekte koji su na bilo koji način uključeni u poslovne procese na osnovu ugovorenih ili drugih obaveza i imaju odobren pristup podacima UC.

Svi gore navedeni dužni su potpisati “Izjavu o prihvatanju PIB-a” i pridržavati se njenih odredbi, u cilju osiguranja pravilnog rada informacionog sistema, a u svrhu očuvanja neprekidnog poslovanja.

PIB se takođe odnosi na cjelokupnu informacionu strukturu UC, uključujući sve resurse informacionog sistema

3. CILJEVI POLITIKE INFORMACIONE BEZBJEDNOSTI

- Postavljanje osnova i odgovornosti za sprovođenje politike informacione bezbjednosti;
- Definisanje metoda i procedura za sprovođenje bezbjednosti i zaštite informacionog sistema UC;
- Osigurati stalnu primjenu PIB-a.

4. POVJERLJIVOST I ZAŠTITA INFORMACIJA

1) Svi zaposleni UC dužni su osigurati podatke i informacije koje obrađuju tokom svog rada. Informaciona bezbjednost počinje redovnim arhiviranjem i skladištenjem podataka, pa do osiguranja pristupa i upravljanja podacima.

2) Informacioni sistem UC zaposleni mogu koristiti samo u poslovne svrhe. Upotreba sistema u lične svrhe nije dozvoljena.

3) Svi zaposleni UC koji imaju pristup ličnim podacima treće strane, moraju raditi prema "Zakonu o zaštiti ličnih podataka" (Službeni list Crne Gore 79/08 i 70/09).

5. ULOGE I ODGOVORNOSTI

- Rukovodstvo UC, Grupa za bezbjednost i standardizaciju i savjetnik za informacionu bezbjednosti (SIB) odgovorni su za ostvarivanje ciljeva politike bezbjednosti informacionih sistema;
- SIB priprema mjesečni izvještaj o informacionoj bezbjednosti i predlaže postupke;
- SIB koordinira aktivnostima vezanim za politiku bezbjednosti, implementaciju i uvođenje poboljšanja. On/Ona je odgovoran/na za ažuriranje dokumentacije koja se odnosi na politiku bezbjednosti;
- Načelnici/Šefovi organizacionih jedinica nadziru sprovođenje politike informacione bezbjednosti u svojim područjima rada i prenose politiku zaposlenima;
- Svi korisnici informacionog sistema moraju biti upoznati sa pravilima bezbjednosti podataka i informacionih sistema kao i sa procedurama koje se odnose na njih. Standardi bezbjednosti moraju se poštovati i sprovoditi;
- Svi zaposleni UC dužni su da odgovorno koriste sve resurse informacionog sistema koji su im dodijeljeni za potrebe izvršavanja radnog procesa;
- Ako zaposleni primijete neovlašćeni pristup informacionom sistemu, moraju obavijestiti svog nadređenog i SIB-a.

6. SPROVOĐENJE POLITIKE INFORMACIONE BEZBJEDNOSTI

6.1 Sigurnosni zahtjevi

- Pravila bezbjednosti za kontrolu opreme i procesa moraju biti u skladu sa procedurama UC;
- Primjena PIB-a mora biti predmet redovne kontrole i nadzora. Ako se ustanovi da se sigurnosni proces može promijeniti ili poboljšati, te izmjene se i uvode.

6.2 Obezbjeđivanje fizičke bezbjednosti

- Fizička bezbjednost mora biti sprovedena kako bi spriječili neovlašćeni pristup, oštećenje i prekide u radu CIS-a;
- Nivo fizičke zaštite informacionih tehnologija mora biti u skladu s vrijednošću štićenih sredstava, rizika i kriterijuma bezbjednosti;
- Resursi informacionog sistema su od ključne važnosti za funkcionisanje cjelokupnog informacionog sistema i moraju biti osigurani od neovlašćenog pristupa i oštećenja. Informatička oprema mora biti smještena u bezbjedne prostorije gdje je pristup dozvoljen samo ovlašćenim osobama;
- Moraju se uvesti sigurnosni mehanizmi koji osiguravaju fizičku bezbjednost, tj sprečavaju krađu, uništenje i druge rizike (požar, poplava, oštećenja tokom prekida napajanja);
- Pristup zaposlenih u UC i drugih pojedinaca resursima informacionog sistema mora biti kontrolisan i nadziran.

6.3 Kontrola pristupa sistemu

- Moraju se uspostaviti procedure za nadzor nad dodjelom prava pristupa sistemu;
- Odgovornosti i procedure koje se odnose na kontrolu bezbjednosti sistema moraju biti dokumentovane;

- Kako bi se identifikovali korisnici i provjerila korisnička prava, mora se uvesti procedura dodjeljivanja korisničkih lozinki i prava, kao i procedura za redovnu promjenu korisničkih lozinki;
- Pristup i način korišćenja sistema od strane korisnika moraju biti kontrolisani i nadzirani. To je naročito važno za stalni nadzor od neovlašćenog pristupa sistemu;
- Pristup lokalnoj mreži (LAN) mora biti kontrolisan i nadziran. Tokom rada na računaru korisnici ne smiju ugroziti sigurnost računarske mreže ili servisa;
- Bezbjednosni mehanizmi moraju uključiti i odgovarajući način odobravanja pristupa korisnicima sa udaljene lokacije.

6.4 Lična odgovornost

- Procedure bezbjednosti moraju biti prezentovane odmah po prijemu novih zaposlenih ili tokom premještanja unutar organizacije, da bi se smanjio rizik od ljudskih grešaka, krađe, prevare i zloupotrebe opreme;
- Prava pristupa informacionom sistemu svakog zaposlenog kome se područje rada promijeni, mora biti promijenjeno i prilagođeno novoj poziciji;
- Svi zaposleni UC moraju biti upoznati s procedurom prijavljivanja događaja koji su vezani za bezbjednost;
- Zaposlenima nije dopušteno dodavati, mijenjati ili uklanjati softvere na korisničkim računarima;
- Zaposlenima nije dozvoljena upotreba nelegalnog softver;
- Bez prethodnog odobrenja nadležne organizacione jedinice, informatička i softverska oprema se ne smije iznositi iz UC, niti mijenjati lokaciju radnog mjesta;
- Prije dodjeljivanja prava na korišćenje resursa informacionog sistema, korisnicima se mora osigurati odgovarajuća obuka.

6.5 Korišćenje računara i softverskih aplikacija

Svi zaposleni u UC su dužni proučiti uputstva o korišćenju radnih stanica/softvera i pratiti i poštovati smjernice o bezbjednosti i zaštiti podataka, kao i o antivirusnoj zaštiti.

6.6 Razvoj Sistema

- Tokom razvoja softvera/aplikacija, razvojno okruženje mora biti odvojeno od testnog i produkcionog okruženja;
- Tokom testiranja softvera/aplikacija, testno okruženje mora biti odvojeno od produkcionog okruženja;
- Standardi i procedure za razvoj, instalaciju i testiranje softvera moraju biti poštovani tokom razvoja. Standardi i procedure moraju biti definisani tako da razvijeni sistem zadovoljava zahtjeve korisnika UC u pogledu kvaliteta, bezbjednosti i funkcionalnosti;
- Razvoj, promjena i nadogradnja informacionog sistema moraju biti u skladu sa standardima. Standardi se moraju redovno razmatrati i prilagođavati prema potrebi;
- Sistem mora biti zaštićen od neovlašćenih izmjena.

7. DOKUMENTACIJA

7.1 Dostupnost dokumentacije

- Procedure za sprovođenje ove politike su dokumentovane u drugim politikama, uputstvima i priručnicima. Sva dodatna dokumenta su sastavni dio ove Politike informacione bezbjednosti;
- Svi zaposleni UC moraju biti upoznati sa politikom informacione bezbjednosti, pratećim dokumentima i lokacijom na kome će ista biti dostupna.

7.2 Promjene

- Sprovođenje politike informacione bezbjednosti je process koji traje. Ažurira se ako postoje promjene u tehnologiji, korišćenju, procedurama, zakonima ili rizicima.
- Savjetnik za informacionu bezbjednost odgovoran je za promjenu politike informacione bezbjednosti i dokumentacije;
- Promjene odobrava rukovodstvo Uprave carina (Direktor).

8. NADZOR NAD POLITIKOM INFORMACIONE BEZBJEDNOSTI I PROCEDURAMA

8.1 Praćenje i poštovanje procedura

U redovnim razmacima (jednom u 6 mjeseci) SIB prati usklađenost implementacije nivoa bezbjednosti sa politikom informacione bezbjednosti. Svi nalazi su dokumentovani i prijavljeni rukovodstvu.

8.2 Kršenje pravila bezbjednosti i prijava kršenja

- Događaji koji nisu u skladu s politikom informaciono bezbjednosti, standardima i uputstvima se tretiraju kao njeno kršenje;
- Svi zaposleni koji uoče takve slučajeve moraju odmah obavijestiti svog nadređenog i SIB-a;
- Ako je potrebno, SIB sprovodi istragu, sačinjava izvještaj i informiše rukovodstvo o nalazima.

8.3 Sankcije u slučaju kršenja pravila politike informacione bezbjednosti

U slučaju kršenja pravila politike informacione bezbjednosti, rukovodioci organizacionih jedinica iniciraju pokretanje aktivnosti za sankcionisanje zaposlenog prema direktoru UC u skladu s važećim zakonodavstvom.

9. PRELAZNE I ZAVRŠNE ODREDBE

Politika informacione bezbjednosti stupa na snagu danom potpisivanja od strane direktora UC i objavljivanja na web portalima UC.

D I R E K T O R
Vladan Joković

CO : 02, a/a