

# ZAKON O INFORMACIONOJ BEZBJEDNOSTI REPUBLIKE SRPSKE

*Službeni glasnik RS br. 70/11*

## Član 1.

Ovim zakonom definiše se informaciona bezbjednost koja se obezbjeđuje primjenom mjera i standarda informacione bezbjednosti.

## Član 2.

(1) Odredbe ovog zakona primjenju:

- a) republički organi,
- b) organi jedinica lokalne samouprave,
- v) pravna lica koja vrše javna ovlašćenja i
- g) druga pravna i fizička lica koja ostvaruju pristup ili postupaju sa podacima u elektronskom obliku republičkih organa, organa jedinica lokalne samouprave i pravnih lica koja vrše javna ovlašćenja.

(2) Odredbe ovoga zakona ne primjenjuju se u onim slučajevima gdje se drugim zakonima propisuje upotreba dokumenta na papiru i na podatke čija se informaciona bezbjednost obezbjeđuje u skladu sa propisima kojima se uređuje tajnost podataka.

## Član 3.

Pojedini izrazi koji se koriste u ovom zakonu imaju sljedeće značenje:

- a) informaciona bezbjednost – stanje povjerljivosti, cjelovitosti i dostupnosti podataka,
- b) podatak – to je informacija, poruka i dokument sačinjen, poslat, primljen, zabilježen, skladišten ili prikazan elektronskim, optičkim ili sličnim sredstvom, uključujući prenos putem interneta i elektronske pošte,
- v) povjerljivost podatka – podatak koji je dostupan samo licima koja su ovlašćena da ostvare pristup ili dalje postupaju sa tim podatkom,
- g) cjelovitost podatka – podrazumijeva očuvanje postojanja, tačnosti i kompletnosti podatka, kao i zaštitu procesa ili programa koji sprečavaju neovlašćeno mijenjanje podatka,
- d) dostupnost podatka – podrazumijeva mogućnost da ovlašćeni korisnici mogu pristupiti podatku uvijek kada za tim imaju potrebu, i
- đ) CERT – Computer Emergency Response Team – to je međunarodno priznat termin, a podrazumijeva posebnu organizacionu jedinicu za djelovanje u hitnim slučajevima, čiji je zadatak koordinacija prevencije i zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema organa i drugih fizičkih i pravnih lica.

#### **Član 4.**

(1) Mjere informacione bezbjednosti su opšta pravila kojima se obezbjeđuje osnovna zaštita podataka na fizičkom, tehničkom i organizacionom nivou.

(2) Vlada Republike Srpske (u daljem tekstu: Vlada) utvrđuje mjere informacione bezbjednosti iz stava 1. ovog člana.

#### **Član 5.**

(1) Mjere iz člana 4. ovog zakona sprovode se u skladu sa standardima informacione bezbjednosti.

(2) Ministar nauke i tehnologije (u daljem tekstu: ministar), na prijedlog Agencije za informaciono društvo Republike Srpske (u daljem tekstu: Agencija), donosi pravilnik kojim se uređuju standardi informacione bezbjednosti.

#### **Član 6.**

(1) Mjere informacione bezbjednosti utvrđuju se u skladu sa vrstom podatka, rizicima za njegovu bezbjednost i vrstom zaštite.

(2) Informaciona bezbjednost obuhvata mjere za:

- a) fizičku zaštitu,
- b) zaštitu podataka i
- v) zaštitu informacionog sistema.

#### **Član 7.**

Fizička zaštita obuhvata zaštitu objekta, prostora i uređaja u kojem se nalaze podaci.

#### **Član 8.**

(1) Zaštita podatka obuhvata prevenciju i otklanjanje štete od gubitka, otkrivanja ili neovlašćene izmjene podataka.

(2) Zaštita iz stava 1. ovog člana odnosi se na:

- a) pravila za postupanje sa podacima,
- b) sadržaj i način vođenja evidencije o izvršenim pristupima podacima i
- v) nadzor koji se tiče bezbjednosti podataka.

#### **Član 9.**

Zaštita informacionog sistema obuhvata zaštitu podataka koji se obrađuju, skladište ili prenose u informacionom sistemu, kao i zaštitu povjerljivosti, cjelovitosti i dostupnosti informacionog sistema u procesu planiranja, projektovanja, izgradnje, upotrebe, održavanja i prestanka rada tog sistema.

#### **Član 10.**

Koordinaciju prevencije i zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema organa i drugih pravnih i fizičkih lica iz člana 2. stav 1. ovog zakona vrši Agencija, preko posebne organizacione jedinice za djelovanje u hitnim slučajevima – CERT.

#### **Član 11.**

(1) Organi i druga pravna i fizička lica iz člana 2. stav 1. ovog zakona mogu organizovati prevenciju i zaštitu svojih informacionih sistema od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti tih sistema.

(2) CERT usklađuje rad organa i drugih pravnih i fizičkih lica iz stava 1. ovog člana.

#### **Član 12.**

Ukoliko nastanu bezbjednosni računarski incidenti na informacionim sistemima organa i drugih pravnih i fizičkih lica iz člana 2. stav 1. ovog zakona, CERT usklađuje postupanje tih organa primjenom mjera informacione bezbjednosti.

#### **Član 13.**

(1) Nadzor nad primjenom ovog zakona vrši Ministarstvo nauke i tehnologije, a stručni nadzor vrši Agencija.

(2) Radi vršenja nadzora, organi i druga pravna i fizička lica iz člana 2. stav 1. ovog zakona dužni su da odgovornom licu organa upravnog i stručnog nadzora omoguće pristup prostoru, računarskoj opremi i uređajima, kao i da bez odlaganja stave na uvid ili dostave potrebne podatke i dokumentaciju u vezi sa predmetom nadzora.

#### **Član 14.**

Vlada će u roku od šest mjeseci od dana stupanja na snagu ovog zakona donijeti uredbu o mjerama informacione bezbjednosti iz člana 4. stav 2. ovog zakona.

#### **Član 15.**

Ministar će u roku od šest mjeseci od dana stupanja na snagu ovog zakona, na prijedlog Agencije, donijeti pravilnik kojim se uređuju standardi informacione bezbjednosti iz člana 5. stav 2. ovog zakona.

#### **Član 16.**

Agencija će u roku od šest mjeseci od dana stupanja na snagu ovog zakona formirati posebnu organizacionu jedinicu za djelovanje u hitnim slučajevima – CERT iz člana 10. ovog zakona.

#### **Član 17.**

Stupanjem na snagu ovog zakona prestaje da važi Zakon o informacionom sistemu Republike Srpske („Službeni glasnik Republike Srpske“, broj 38/98).

#### **Član 18.**

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u „Službenom glasniku Republike Srpske“.