Uredba o mjerama informacione bezbjednosti

Uredba je objavljena u "Službenom listu CG", br. 58/2010 i 55/2015.

I. OSNOVNE ODREDBE

Predmet

Član 1

Ovom uredbom utvrđuju se mjere informacione bezbjednosti kojima se obezbjeđuje osnovna zaštita podataka na fizičkom, tehničkom i organizacionom nivou.

Obaveza primjene

Član 2

Mjere iz člana 1 ove uredbe odnose se na državne organe, organe državne uprave, organe jedinica lokalne samouprave, pravna lica sa javnim ovlašćenjima (u daljem tekstu: organi) i druga pravna i fizička lica koja ostvaruju pristup ili postupaju sa podacima.

Značenje izraza

Član 3

Pojedini izrazi upotrijebljeni u ovoj uredbi imaju sljedeće značenje:

1) **hardver** je fizička komponenta informacionog sistema;

2) **kriptografska zaštita** je sistem zaštite podataka i informacionih sistema koji osigurava siguran prenos podataka kroz računarsku i telekomunikacionu mrežu;

3) **informatički medij** je svaki medij na kojem je moguće prenositi ili skladištiti podatke u elektronskom obliku;

4) **bezbjedno skladište** je sef, kasa ili drugi prostor za skladištenje podataka opremljen uređajem koji sprječava neovlašćeni pristup uskladištenim podacima;

5) **softver** je svaki operativni sistem, program, korisnička i servisna aplikacija;

6) **rizik** je potencijalni uzrok koji može nanijeti štetu podatku ili informacionom sistemu u kojem se koriste podaci;

7) **bezbjedna lokacija** je mjesto za čuvanje podataka skladištenih na informatičkom mediju u ili izvan radnih prostorija organa, pravnog ili fizičkog lica iz člana 2 ove uredbe, opremljen tehničkim uređajima, kojima se sprječava neovlašćeni pristup uređajima i podacima;

8) **administrativna zona** je prostor ili prostorija u objektu u kojem se čuvaju podaci i uređaji na kojima su smješteni podaci i koji zahtijeva odgovarajuću fizičku zaštitu;

9) **kriptovana zaštita** podataka je primjena programskih rješenja ili uređaja za zaštitu podataka koji osiguravaju cjelovitost, povjerljivost i dostupnost podataka;

10) **ključni informacioni sistem** je informacioni sistem od čijeg funkcionisanja zavisi vršenje ključnih poslova iz nadležnosti organa;

11) **rezervna lokacija** je lokacija za čuvanje podataka i uređaja na kojima su smješteni podaci koji se vode u ključnim informacionim sistemima, koja u slučaju vanrednih situacija preuzima funkcionisanje ključnih informacionih sistema.

II. FIZIČKA ZAŠTITA

Vrste mjera

Član 4

Mjere informacione bezbjednosti fizičke zaštite su:

1) uspostavljanje administrativne zone;

2) izrada plana fizičke zaštite;

3) procjena efikasnosti mjera fizičke zaštite;

4) kontrola lica;

5) skladištenje podataka;

6) fizička zaštita informacionih sistema.

Cilj sprovođenja mjera

Član 5

Mjere informacione bezbjednosti fizičke zaštite sprovode se radi:

- sprječavanja neovlašćenog ili nasilnog ulaska lica u objekte i prostorije u kojima se nalaze podaci odnosno uređaji sa podacima;
- sprječavanja i otkrivanja zloupotreba podataka od strane zaposlenih;
- otkrivanja i reagovanja na rizike.

Kriterijumi za određivanje mjera

Član 6

Mjere informacione bezbjednosti fizičke zaštite određuju se zavisno od vrste, broja, oblika i načina skladištenja podataka, ovlašćenja za pristup podacima, kao i bezbjednosne procjene mogućih rizika.

Uspostavljanje administrativne zone

Član 7

Administrativna zona se uspostavlja za korišćenje podataka u kontrolisanom, vidljivo označenom prostoru unutar kojeg je moguće kontrolisati pristup lica.

Izrada plana fizičke zaštite

Član 8

Organi, pravna i fizička lica iz člana 2 ove uredbe, za objekat ili prostor u kojem imaju pristup, odnosno postupaju sa podacima, izrađuju plan fizičke zaštite kojim se utvrđuje potreba sprovođenja mjera fizičke zaštite, u skladu sa standardima informacione bezbjednosti.

Procjena efikasnosti mjera fizičke zaštite

Član 9

Organi, pravna i fizička lica iz člana 2 ove uredbe, najmanje jednom godišnje, procjenjuju efikasnost mjera informacione bezbjednosti fizičke zaštite objekata i prostorija u kojima se nalaze podaci, kao i kad dođe do promjene namjene lokacije ili elemenata u informacionom sistemu.

Kontrola lica

Član 10

Organi, pravna i fizička lica iz člana 2 ove uredbe, dužni su da sprovode kontrolu lica na ulazima i izlazima iz objekta ili prostora u kojima se nalaze podaci i o tome vode evidenciju, radi sprječavanja neovlašćenog iznošenja podataka ili sprječavanja unošenja nedozvoljenih predmeta, kojima se može ugroziti bezbjednost podataka.

Skladištenje podataka

Član 11

Podatak se skladišti na odgovarajućem informatičkom mediju, koji se odlaže i čuva u bezbjednom skladištu.

Fizička zaštita informacionog sistema

Član 12

Prostor u kojem se nalaze računari za vođenje baze podataka i centralni računar informacionog sistema (serveri), mrežna ili komunikaciona oprema informacionog sistema, organizuje se kao administrativna zona.

III. ZAŠTITA PODATAKA

Mehanizmi za zaštitu podataka

Član 13

Računar za vođenje baze podataka i centralni računar informacionog sistema (server) mora biti opremljen:

1) sistemom za bezbjedno prijavljivanje za rad sa mogućnošću evidentiranja ostvarenih pristupa, kako bi se pristup serveru mogao kontrolisati i ograničiti;

2) mehanizmom za sprječavanje neovlašćenog iznošenja i unošenja podataka upotrebom prenosivih informatičkih medija, komunikacionih priključaka i priključaka za ispis podataka;

3) mehanizmom zaštite od računarskih virusa i drugih štetnih programa;

4) mehanizmom zaštite podataka ključnih informacionih sistema koji omogućava sinhronizaciju podataka na rezervnoj lokaciji.

Pristup bazi podataka

Član 14

Pristup bazi podataka dozvoljen je samo licima zaduženim za održavanje i razvoj informacionog sistema.

Pristup telekomunikacionom, računarskom i aplikativnom sistemu

Član 15

Pristup telekomunikacionom, računarskom i aplikativnom sistemu za obradu podataka, dozvoljen je uz upotrebu odgovarajućeg korisničkog imena i pripadajuće lozinke, odnosno upotrebu digitalnog certifikata.

Korisničko ime i pripadajuća lozinka ne smiju se otkriti i dati na upotrebu drugom licu.

Upravljanje sistemom korisničkog pristupa

Član 16

Upravljanje sistemom korisničkog pristupa podrazumijeva razvoj, primjenu i održavanje informacionog sistema, na način koji omogućava jednoznačno identifikovanje i pouzdano garantovanje identiteta korisnika.

Obaveza skladištenja podataka

Član 17

Organi, pravna i fizička lica iz člana 2 ove uredbe dužni su da skladište sve podatke iz informacionih sistema na informatičke medije upotrebom metoda koji garantuju bezbjednost, povjerljivost, cjelovitost i dostupnost uskladištenih podataka.

Dnevno, sedmično, mjesečno i godišnje skladištenje podataka

Član 18

Baze podataka obavezno se skladište na prenosive informatičke medije najmanje jednom dnevno, sedmično, mjesečno i godišnje, za potrebe obnove baze podataka.

Podaci informacionog sistema skladište se u onoliko dnevnih primjeraka koliko ima radnih dana u sedmici.

Sedmično skladištenje podataka informacionog sistema vrši se posljednjeg radnog dana u sedmici, nakon sprovođenja dnevnog skladištenja podataka, u onoliko sedmičnih primjeraka koliko u mjesecu ima posljednjih radnih dana u sedmici.

Mjesečno skladištenje podataka informacionog sistema vrši se posljednjeg radnog dana u mjesecu, za svaki mjesec posebno.

Godišnje skladištenje podataka informacionog sistema vrši se posljednjeg radnog dana u godini.

Svaki primjerak godišnje uskladištenih podataka čuva se za vrijeme određeno propisima kojima se uređuje arhivska djelatnost.

Svaki primjerak prenosivog informatičkog medija sa uskladištenim podacima mora biti označen brojem, vrstom (dnevno, sedmično, mjesečno, godišnje), datumom skladištenja, kao i imenom lica koje je izvršilo skladištenje podataka.

Organi, pravna i fizička lica iz člana 2 ove uredbe vode evidenciju informatičkih medija na kojima su podaci uskladišteni.

Lokacija za odlaganje uskladištenih podataka

Član 19

Podaci informacionog sistema dnevno uskladišteni na informatičke medije odlažu se u najmanje jedno bezbjedno skladište u radnoj prostoriji organa, pravnog ili fizičkog lica iz člana 2 ove uredbe ili na drugoj bezbjednoj lokaciji.

Podaci informacionog sistema sedmično, mjesečno i godišnje uskladišteni na informatičke medije odlažu se na bezbjednu lokaciju.

Provjera ispravnosti sigurnosnih kopija

Član 20

Upotrebljivost sigurnosne kopije podataka provjerava se najmanje svakih šest mjeseci, uz provjeru postupka povraćaja baza podataka uskladištenih na informatičkom mediju, tako da vraćeni podaci nakon izvršene provjere budu cjeloviti, povjerljivi i dostupni za upotrebu.

Vremenski termini provjere kvaliteta medija

Član 21

Podaci uskladišteni godišnje na informatičkom mediju moraju se obnoviti nakon isteka polovine garantovanog roka trajanja zapisa na toj vrsti medija.

Sistem kriptovane zaštite podataka u prenosu informacionim i telekomunikacionim sistemom

Član 22

Organi, pravna i fizička lica iz člana 2 ove uredbe uspostavljaju sistem kriptovane zaštite podataka u prenosu tih podataka informacionim i telekomunikacionim sistemom.

IV. ZAŠTITA INFORMACIONOG SISTEMA

Smještaj, postavljanje i ugradnja servera, računara i računarske mreže

Član 23

Računar za vođenje baze podataka i centralni računar informacionog sistema (server) i računarsku mrežu postavlja i ugrađuje stručno lice, u skladu sa projektnom dokumentacijom, važećim normama, standardima i tehničkim uputstvima.

Po jedan primjerak projektne dokumentacije iz stava 1 ovog člana čuva se u radnim prostorijama organa, pravnog ili fizičkog lica iz člana 2 ove uredbe, na bezbjednom mjestu, a dostavlja se na uvid na zahtjev organa državne uprave nadležnog za poslove informacionog društva (u daljem tekstu: nadležni organ).

Kontrola povezivanja informacionih sistema

Član 24

Kontrola povezivanja informacionih sistema obuhvata definisanje uslova povezivanja informacionih sistema, kao i evidentiranje i nadzor povezivanja.

Kontrola upotrebe informacionog sistema

Član 25

Kontrola upotrebe informacionog sistema podrazumijeva evidentiranje aktivnosti korisnika informacionog sistema, kao i mjere za sprječavanje zloupotrebe informacionog sistema kroz instaliranje sistema za otkrivanje neovlašćenog upada u računarsku mrežu, definisanje, pregledanje i analiziranje zapisa rada informacionog sistema i sprovođenje analiza ranjivosti informacionog sistema.

Evidencija, praćenje pristupa i pokušaja neovlašćenog pristupa sistemu

Član 26

Svaki pristup informacionom sistemu za obradu i skladištenje podataka mora biti automatski zabilježen korisničkim imenom, datumom i vremenom prijave i odjave.

Svaki pokušaj neovlašćenog pristupa informacionom sistemu mora biti automatski zabilježen korisničkim imenom, datumom i vremenom, a ako je to moguće i mjestom sa kojeg je takav pristup pokušan.

Lice iz člana 14 ove uredbe dužno je da obavijesti starješinu organa, rukovodioca pravnog lica, odnosno fizičko lice o svakom pokušaju neovlašćenog pristupa informacionom sistemu.

Mjere zaštite od požara

Član 27

Informacioni sistem mora biti smješten u prostorijama koje imaju uređaje za otkrivanje požara i automatsko obavještavanje o izbijanju požara.

Prostorije u kojima je smješten informacioni sistem moraju imati uređaje za gašenje požara, a u blizini, ispred i u tim prostorijama, na vidljivim i lako uočljivim mjestima moraju biti istaknuta uputstva o postupanju u slučaju izbijanja požara.

Mjere zaštite od električnog i magnetskog polja, elektrostatičkog elektriciteta i jonizirajućeg zračenja

Član 28

U blizini računarske i telekomunikacione opreme ne smije se postavljati:

1) izvor jakog električnog ili magnetskog polja;
2) izvor elektrostatičkog elektriciteta;
3) izvor jonizirajućeg zračenja.

Mjere zaštite od vlage, hladnoće i toplote

Član 29

U prostorijama u kojima je smješten informacioni sistem mora se održavati odgovarajuća vlažnost vazduha i temperatura.

Mjere zaštite od nagrizajuće i lako zapaljive tečnosti, eksplozivnih sredstava i sličnih jedinjenja

Član 30

U prostorijama i u blizini prostorija u kojima je smještena oprema informacionog sistema, ne smiju se nalaziti nagrizajuća i lakozapaljiva tečnost, eksplozivna sredstva i slična opasna ili štetna hemijska jedinjenja.

Primjena kriptografske zaštite

Član 31

Povjerljivost, cjelovitost i dostupnost podataka obezbjeđuje se korišćenjem kriptografskih metoda odobrenih od strane nadležnog organa.

Uspostavljanje bezbjednosnih pravila i edukacija zaposlenih

Član 32

Organi, pravna i fizička lica iz člana 2 ove uredbe uspostavljaju bezbjednosna pravila radi obezbjeđivanja informacione bezbjednosti podataka kojima ta lica imaju pristup, odnosno koja postupaju sa njima.

Bezbjednosna pravila iz člana 1 ove uredbe podrazumijevaju:

1) interna pravila za zaposlene;

2) edukaciju i stručno usavršavanje zaposlenih.

Planiranje djelovanja i postupanje u vanrednim situacijama

Član 33

Planiranje djelovanja u vanrednim situacijama podrazumijeva analizu potencijalnih rizika u radu informacionog sistema i utvrđivanje postupaka za rješavanje tih rizika, kao i drugih metoda korišćenja resursa informacionog sistema u slučaju nedostupnosti informacionog sistema, a u cilju održavanja neprekidnog funkcionisanja, odnosno poslovanja organa, pravnog i fizičkog lica iz člana 2 ove uredbe.

Planiranje djelovanja u vanrednim situacijama obuhvata:

1) izradu plana neprekidnog funkcionisanja, odnosno poslovanja organa, pravnog i fizičkog lica iz člana 2 ove uredbe;

2) izradu procedura za postupanje u slučaju incidenata.

Plan neprekidnog poslovanja

Član 34

Plan neprekidnog funkcionisanja, odnosno poslovanja obuhvata identifikovanje ključnih informacionih sistema i uspostavljanje rezervne lokacije, uspostavljanje i testiranje adekvatne procedure bezbjednog skladištenja podataka, radi vraćanja informacionog sistema i podataka u prvobitno stanje nakon incidenta, koji podrazumijeva ispad informacionog sistema, prirodne nepogode i djelovanje računarskih virusa.

Izrada procedura za postupanje u slučaju incidenata

Član 35

Izrada procedura za postupanje u slučaju incidenta podrazumijeva planiranje i definisanje aktivnosti, sprječavanja, detekcije i oporavka od posljedica incidenta, koji utiču na povjerljivost, cjelovitost i dostupnost podatka ili informacionog sistema, uključujući i izvještavanje o incidentima.

Izvještavanje o incidentima iz stava 1 ovog člana, podrazumijeva dostavljanje osnovnih podataka o incidentu posebnoj organizacionoj jedinici u nadležnom organu.

V. UPRAVLjANjE RIZIKOM INFORMACIONE BEZBJEDNOSTI

Upravljanje rizikom

Član 36

Upravljanje rizikom informacione bezbjednosti podrazumijeva planiranje, organizovanje i usmjeravanje aktivnosti, radi obezbjeđivanja uslova da rizici ne ugroze neprekidno funkcionisanje, odnosno poslovanje organa, pravnog i fizičkog lica iz člana 2 ove uredbe.

Planiranje iz stava 1 ovog člana podrazumijeva utvrđivanje stepena prihvatljivosti rizika, radi njegovog prihvatanja, smanjivanja ili izbjegavanja (u daljem tekstu: analiza rizika).

Prihvatanje, smanjivanje i izbjegavanje rizika

Član 37

Rizik se može prihvatiti ukoliko bi nastala šteta bila manja od štete koja bi nastala usljed nesprovođenja određene aktivnosti.

Smanjivanje rizika sprovodi se primjenom mjera definisanih u planu aktivnosti iz člana 38 ove uredbe, radi sprječavanja

uništenja, otuđenja, gubitka i neovlašćenog pristupa podacima.

Izbjegavanje rizika podrazumijeva preduzimanje organizacionih i drugih neophodnih mjera u cilju izbjegavanja radnji koje bi mogle izazvati rizik.

Plan aktivnosti

Član 38

Nakon analize rizika, organi, pravna i fizička lica iz člana 2 ove uredbe, obavezni su da sačine plan aktivnosti u kojem se utvrđuje sprovođenje potrebnih mjera.

Preispitivanje plana

Član 39

Rezultati analize rizika redovno se preispituju, saglasno potrebama organa, pravnog i fizičkog lica iz člana 2 ove uredbe, uslovljenim unutrašnjim ili vanjskim promjenama.

VI. ZAVRŠNA ODREDBA

Stupanje na snagu

Član 40

Ova uredba stupa na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore".