

Prečišćeni tekst Pravilnika o načinu i rokovima za sprovođenje mjera zaštite sigurnosti i integriteta elektronskih komunikacionih mreža i usluga obuhvata sljedeće propise:

1. Pravilnik o načinu i rokovima za sprovođenje mjera zaštite sigurnosti i integriteta elektronskih komunikacionih mreža i usluga ("Službeni list Crne Gore", br. 041/15 od 28.07.2015),
2. Pravilnik o izmjenama Pravilnika o načinu i rokovima za sprovođenje mjera zaštite sigurnosti i integriteta elektronskih komunikacionih mreža i usluga ("Službeni list Crne Gore", br. 081/16 od 28.12.2016), u kojima je naznačen njihov dan stupanja na snagu.

## **PRAVILNIK**

# **O NAČINU I ROKOVIMA ZA SPROVOĐENJE MJERA ZAŠTITE SIGURNOSTI I INTEGRITETA ELEKTRONSKIH KOMUNIKACIONIH MREŽA I USLUGA**

("Službeni list Crne Gore", br. 041/15 od 28.07.2015, 081/16 od 28.12.2016)

### **Sadržaj Pravilnika**

#### **Član 1**

Ovim pravilnikom propisuju se način i rokovi za sprovođenje mjera zaštite sigurnosti i integriteta elektronskih komunikacionih mreža i usluga, kao i način obavještanja o povredi sigurnosti i integriteta elektronskih komunikacionih mreža i usluga.

### **Značenje izraza**

#### **Član 2**

Pojedini pojmovi u smislu ovog pravilnika imaju sljedeće značenje:

1. Integritet mreže: osobina mreže da održi specificirane parametre u dijelu performansi i funkcionalnosti.
2. Kritična sredstva: elementi mreže i infrastruktura čiji bi prekid rada, vjerovatno imao direktan i značajan uticaj na sigurnost mreža i usluga ili direktan uticaj na procesuiranje ličnih podataka.
3. Prijetnja: događaj ili okolnost koja može dovesti do sigurnosnog incidenta.
4. Sigurnosne mjere: skup administrativnih, tehničkih i fizičkih zahtjeva za procese, rad i izmjene u elektronskoj komunikacionoj mreži, u svrhu osiguranja nesmetanog pristupa i upotrebe elektronskih komunikacionih mreža, kao i sigurnosti i integriteta podataka sačuvanih u elektronskoj komunikacionoj mreži.
5. Sigurnosni incident: jedan ili više neželjenih ili neočekivanih događaja koji mogu uticati na sigurnost i integritet mreža i usluga ili sigurnost, integritet i obradu ličnih podataka.

### **Mjere za zaštitu sigurnosti i integriteta mreža i usluga**

#### **Član 3**

Mjere za obezbjeđenje integriteta javne elektronske komunikacione mreže, obezbjeđenja neprekidnog pružanja javnih elektronskih komunikacionih usluga, obezbjeđenja sigurnosti ličnih podataka, obezbjeđenja odgovora na sigurnosne incidente, ublažavanja uticaja sigurnosnih incidenata na rad svoje elektronske komunikacione mreže i sa njom povezanih mreža, ublažavanja uticaja prijetnji i sigurnosnih incidenata na korisnike elektronskih komunikacionih usluga, zaštite korisnika od zlonamjernih aktivnosti, elektronskih sabotaza, prevara trećih lica i zloupotreba bilo koje vrste (u daljem tekstu sigurnosne mjere), operator je dužan da primijeni u sljedećim oblastima:

- Upravljanje rizikom;
- Sigurnost ljudskih resursa;
- Sigurnost sistema i objekata;
- Upravljanje operacijama;
- Upravljanje incidentima;
- Upravljanje kontinuitetom poslovanja;
- Nadzor, revizija i testiranje.

U okviru svake oblasti iz stava 1 ovog člana operator je dužan da ispuni odgovarajuće sigurnosne ciljeve, preduzimanjem sigurnosnih mjera koje su navedene u Prilogu 1 ovog pravilnika.

Sigurnosne mjere iz Priloga 1 ovog pravilnika operator je dužan da sprovede u skladu sa odgovarajućim standardima, koji su navedeni u Prilogu 2 ovog pravilnika.

Operator koji pruža usluge telefonskih poziva i pristupa Internetu u fiksnoj elektronskoj komunikacionoj mreži i usluge u mobilnoj elektronskoj komunikacionoj mreži, za više od 10000 korisnika, dužan je da, izgradnjom georedundantne konfiguracije odgovarajućih elemenata mreže i sistema (Disaster Recovery Site) na teritoriji Crne Gore, obezbijedi neprekidnost pružanja telefonske usluge, usluge SMS-a i usluge pristupa Internetu.

## **Praćenje sprovođenja mjera za zaštitu sigurnosti i integriteta mreža i usluga**

### **Član 4**

Operator je dužan da, u cilju praćenja sprovođenja sigurnosnih mjera, Agenciji za elektronske komunikacije i poštansku djelatnost (u daljem tekstu Agencija) dostavi:

- 1) dokumenta kojima se definišu sigurnosne mjere iz člana 3, i postupci za njihovo sprovođenje, u roku 7 dana od njihovog usvajanja;
- 2) podatke o licu odgovornom za sprovođenje sigurnosnih mjera iz stava 1 člana 3 ovog pravilnika, u roku 7 dana od stupanja ovog pravilnika na snagu;
- 3) podatke o mjerama nadzora sigurnosti i integriteta mreža i usluga operatora od strane organa državne uprave nadležnog za prevenciju i zaštitu rizika bezbjednosti informacionih sistema odnosno organa uprave nadležnog za oblast računarskog kriminala, u roku 7 dana od vršenja nadzora;
- 4) izvještaje o interno sprovedenim kontrolama sigurnosti i integriteta elektronskih komunikacionih mreža i usluga i datim preporukama, u roku 7 dana od prijema izvještaja o sprovedenim kontrolama;
- 5) obavještenja i izvještaje o sigurnosnim incidentima.

Agencija, ili lica angažovana od strane Agencije, će vršiti kontrolu sprovođenja sigurnosnih mjera iz člana 3 ovog pravilnika.

## **Obavještanje o sigurnosnim incidentima**

### **Član 5**

Operator je dužan da, pisanim putem obavijesti Agenciju o sigurnosnom incidentu koji je doveo do prekida u pružanju telefonske usluge, usluge pristupa Internetu ili usluge distribucije audio-vizuelnih medijskih sadržaja u fiksnoj mreži za više od 1000 korisnika, a prekida u pružanju telefonske usluge i usluge SMS-a u mobilnoj mreži na teritoriji većoj od 46 km<sup>2</sup> odnosno povrede sigurnosti ličnih podataka korisnika u fiksni i mobilni mrežama.

Operator je dužan da obavještenje o sigurnosnom incidentu iz stava 1 ovog člana dostavi Agenciji, u roku od 1 sata nakon pojave sigurnosnog incidenta, u skladu sa Prilogom 3 koji je sastavni dio ovog pravilnika.

Operator je dužan da, pisanim putem Agenciji dostavi izvještaj o sigurnosnom incidentu, koji je značajnije uticao na rad javnih elektronskih komunikacionih mreža ili pružanje elektronskih komunikacionih usluga, u skladu sa kriterijumima za izvještanje iz Priloga 4 koji je sastavni dio ovog pravilnika.

Operator je dužan da izvještaj o sigurnosnom incidentu iz stava 3 ovog člana dostavi Agenciji, u roku od 3 radna dana od otklanjanja sigurnosnog incidenta, u skladu sa Prilogom 5, koji je sastavni dio ovog pravilnika.

Operator može obavijestiti Agenciju i o drugim važnim sigurnosnim incidentima koji se odnose na sigurnost i integritet javnih elektronskih komunikacionih mreža i usluga, a koji nisu obuhvaćeni sigurnosnim incidentima iz stavova 1. i 3. ovog člana.

Operator je dužan da odmah obavijesti druge operatore u slučaju da povreda sigurnosti i integriteta njegove mreže može značajnije uticati na rad sa njom povezanih mreža.

## **Prelazne i završne odredbe**

### **Član 6**

Operator je dužan da svoj rad uskladi sa ovim pravilnikom u roku od šest mjeseci, a sa odredbom člana 3 stav 4 ovog pravilnika u roku od 24 mjeseca od dana stupanja pravilnika na snagu.

## **Stupanje na snagu**

### **Član 7**

Ovaj Pravilnik stupa na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore".

PRILOG 1: Sigurnosne mjere

| OBLAŠT SIGURNOSTI                    | SIGURNOSNE MJERE  |
|--------------------------------------|---|
| Upravljanje rizikom                  | <p>Uspostavljanje i održavanje odgovarajućih procedura informacione sigurnosti koja se odnosi na sigurnost mreža, usluga i procesuiranja ličnih podataka; (<b>Information security policy</b>)</p> <p>Uspostavljanje i održavanje odgovarajućeg okvira za upravljanje rizikom, koji služi za identifikaciju i adresiranje rizika za mreže, usluge i procesuiranje ličnih podataka; (<b>Governance and risk management</b>)</p> <p>Uspostavljanje i održavanje odgovarajuće strukture sigurnosti sa ulogama i odgovornostima; (<b>Security roles and responsibilities</b>)</p> <p>Uspostavljanje i održavanje procedura sa zahtjevima koji se tiču sigurnosti za ugovore sa trećim stranama, kako bi se obezbijedilo da zavisnost od trećih strana ne utiče negativno na sigurnost mreža, usluga i procesuiranja ličnih podataka (<b>Security of third party assets</b>).</p>  |
| Sigurnost ljudskih resursa           | <p>Obezbijediti odgovarajuću provjeru osoblja (zaposlenih, ugovarača i korisnika treće strane) kada je to potrebno za njihove dužnosti i odgovornosti (<b>Background checks</b>);</p> <p>Obezbijediti da osoblje ima dovoljno znanja o sigurnosti, a takođe, obezbijediti i redovnu obuku na temu sigurnosti (<b>Security knowledge and training</b>);</p> <p>Uspostaviti i održavati odgovarajuće procedure za upravljanje promjene osoblja ili za promjene njihovih uloga i odgovornosti (<b>Personnel changes</b>);</p> <p>Uspostaviti i održavati disciplinske procedure za zaposlene koji prekrše politike sigurnosti ili imati šire procedure koje pokrivaju sigurnosne prekršaje čije kršenje je izazvalo osoblje. (<b>Handling violations</b>);</p>   |
| Sigurnost sistema i objekata         | <p>Uspostaviti i održavati odgovarajuću fizičku sigurnost i sigurnost uslova u objektima (<b>Physical and environmental security of facilities</b>);</p> <p>Uspostaviti i održavati odgovarajuću sigurnost snadbijevanja (električnom energijom, naftnim derivatima-gorivom, klimatizacijom itd) za objekte (<b>Security of supplies</b>);</p> <p>Uspostaviti i održavati odgovarajuće (logičke) kontrole pristupa mreži i informacionim sistemima, kako bi se spriječio nedozvoljeni pristup, izmjena ili brisanje podataka na tim sistemima (<b>Access control to network and information systems</b>);</p> <p>Uspostaviti i održavati integritet mreže i informacionih sistema, radi zaštite od trojanaca, "code injections" i drugih malvera koji mogu promijeniti njihovu funkcionalnost (<b>Integrity of network and information systems</b>);</p> <p>Uspostaviti i održavati odgovarajuće procedure o povjerljivosti i integritetu sadržaja komunikacija i metapodataka o komunikacijama (<b>Confidentiality of communications</b>).</p> |
| Upravljanje operacijama              | <p>Uspostaviti i održavati operativne procedure za funkcionisanje kritičnih mrežnih i informacionih sistema od strane osoblja (<b>Operational procedures</b>);</p> <p>Uspostaviti procedure za upravljanje promjenama za kritične mrežne i informacione sisteme, kako bi se umanjili incidenti koji su prouzrokovani promjenama (<b>Change management</b>);</p> <p>Uspostaviti i održavati procedure za upravljanje sredstvima i kontrolu konfiguracije u cilju upravljanja raspoloživošću kritičnih sredstava i konfiguracija kritičnih mrežnih i informacionih sistema (<b>Asset management</b>).</p>   |
| Upravljanje incidentima              | <p>Uspostaviti i održavati procedure za upravljanje sigurnosnim incidentima, kao i njihovo prosljeđivanje prema odgovarajućem osoblju (<b>Incident management procedures</b>);</p> <p>Uspostaviti i održavati odgovarajuće kapacitete za detekciju sigurnosnih incidentata (<b>Incident detection capability</b>);</p> <p>Uspostaviti i održavati odgovarajuće procedure za izvještavanje i objavljivanje o incidentima, uzimajući u obzir nacionalno zakonodavstvo za izvještavanje državnih institucija o incidentima (<b>Incident reporting and communication</b>);</p>  |
| Upravljanje kontinuitetom poslovanja | <p>Uspostaviti i održavati planove za vanredne situacije i strategiju za obezbjeđenje kontinuiteta u pružanju mreža i usluga (<b>Service continuity strategy and contingency plans</b>);</p>  |

|                               |   |
|-------------------------------|---|
|                               | Uspostaviti i održavati odgovarajuće "disaster recovery" kapacitete za vraćanje u rad mreža i usluga u slučaju prirodnih i/ili velikih katastrofa ( <b>Disaster recovery capabilities</b> ).  |
| Nadzor, revizija i testiranje | Uspostaviti i održavati sisteme i funkcije nadzora i logovanja kritičnih mrežnih i komunikacionih sistema ( <b>Monitoring and logging policies</b> );<br>Uspostaviti i održavati procedure za testiranje i uvježbavanje planova za vanredne situacije i obebeđivanje backupa, kada je potrebno u sardnji sa trećim stranama ( <b>Exercise contingency plans</b> );<br>Uspostavljanje i održavanje procedura za testiranje mrežnih i informacionih sistema, posebno u slučajevima povezivanja sa novom mrežom ili informacionim sistemom ( <b>Network and information systems testing</b> );<br>Uspostavljanje i održavanje odgovarajućih procedura za obavljanje sigurnosnih procjena i testova mrežnih i informacionih sistema ( <b>Security assessments</b> );<br>Uspostaviti i održavati procedure za nadzor usklađenosti sa standardima i zakonskim obavezama ( <b>Compliance monitoring</b> ). |

**PRILOG 2: Standardi za sprovođenje sigurnosnih mjera**

| OBLAST SIGURNOSTI                    | REFERENTNI STANDARDI   |
|--------------------------------------|--|
| Upravljanje rizikom                  | MEST ISO/IEC 27001<br>MEST ISO/IEC 27002<br>MEST ISO/IEC 27005<br>MEST ISO/IEC 27011 |
| Sigurnost ljudskih resursa           | MEST ISO/IEC 27001<br>MEST ISO/IEC 27002<br>MEST ISO/IEC 27011                       |
| Sigurnost sistema i objekata         | MEST ISO/IEC 27001<br>MEST ISO/IEC 27002<br>MEST ISO/IEC 27011                       |
| Upravljanje operacijama              | MEST ISO/IEC 27001<br>MEST ISO/IEC 27002<br>MEST ISO/IEC 27011                       |
| Upravljanje incidentima              | MEST ISO/IEC 27001<br>MEST ISO/IEC 27002<br>MEST ISO/IEC 27011                       |
| Upravljanje kontinuitetom poslovanja | ISO/IEC 22301<br>MEST ISO/IEC 27011  |
| Nadzor, revizija i testiranje        | MEST ISO/IEC 27001<br>MEST ISO/IEC 27002<br>MEST ISO/IEC 27011                       |

**PRILOG 3:**

**Obavještenje o sigurnosnom incidentu**

| Operator   |  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
|--|--|--|----------------------------|--------------------|-------|------------------|-------|---------------------|-------|-------------------|-------|--------------------------|-------|----------------------------|-------|--------|-------|
| Datum i vrijeme nastanka sigurnosnog incidenta   |  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Datum i vrijeme utvrđivanja sigurnosnog incidenta  |  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Način utvrđivanja sigurnosnog incidenta  |  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Vrsta usluge koju obuhvata sigurnosni incident   | Fiksna telefonija: <input type="checkbox"/> PSTN <input type="checkbox"/> IMS <input type="checkbox"/> VoIP <input type="checkbox"/> DRUGO _____<br>Fiksni Internet: <input type="checkbox"/> xDSL <input type="checkbox"/> FTTx <input type="checkbox"/> KDS <input type="checkbox"/> DRUGO _____<br>Mobilna telefonija: <input type="checkbox"/> GSM <input type="checkbox"/> UMTS <input type="checkbox"/> LTE <input type="checkbox"/> DRUGO _____<br>Mobilni Internet: <input type="checkbox"/> GPRS/EDGE <input type="checkbox"/> UMTS <input type="checkbox"/> LTE <input type="checkbox"/> DRUGO _____<br>Zemaljska radiodifuzija: <input type="checkbox"/> Zemaljska TV <input type="checkbox"/> Zemaljski radio<br>Distribucija AVM sadržaja: <input type="checkbox"/> KDS <input type="checkbox"/> IPTV <input type="checkbox"/> Satelitski <input type="checkbox"/> MMDS <input type="checkbox"/> DRUGO<br>Drugo _____ |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Opis sigurnosnog incidenta   |  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Broj obuhvaćenih korisnika   | <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;"></th> <th style="text-align: center;">BROJ OBUHVAĆENIH KORISNIKA</th> </tr> </thead> <tbody> <tr> <td>Fiksna telefonija:</td> <td style="text-align: center;">_____</td> </tr> <tr> <td>Fiksni Internet:</td> <td style="text-align: center;">_____</td> </tr> <tr> <td>Mobilna telefonija:</td> <td style="text-align: center;">_____</td> </tr> <tr> <td>Mobilni Internet:</td> <td style="text-align: center;">_____</td> </tr> <tr> <td>Zemaljska radiodifuzija:</td> <td style="text-align: center;">_____</td> </tr> <tr> <td>Distribucija AVM sadržaja:</td> <td style="text-align: center;">_____</td> </tr> <tr> <td>Drugo:</td> <td style="text-align: center;">_____</td> </tr> </tbody> </table>  |  | BROJ OBUHVAĆENIH KORISNIKA | Fiksna telefonija: | _____ | Fiksni Internet: | _____ | Mobilna telefonija: | _____ | Mobilni Internet: | _____ | Zemaljska radiodifuzija: | _____ | Distribucija AVM sadržaja: | _____ | Drugo: | _____ |
|  | BROJ OBUHVAĆENIH KORISNIKA   |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Fiksna telefonija:   | _____  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Fiksni Internet:   | _____  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Mobilna telefonija:  | _____  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Mobilni Internet:  | _____  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Zemaljska radiodifuzija:   | _____  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Distribucija AVM sadržaja:   | _____  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Drugo:   | _____  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Uticaj na hitne službe   | <input type="checkbox"/> DA <input type="checkbox"/> NE  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Uticaj na interkonekciju (u zemlji i inostranstvu)   | <input type="checkbox"/> DA <input type="checkbox"/> NE  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Da li je došlo do povrede ličnih podataka korisnika?   | <input type="checkbox"/> DA <input type="checkbox"/> NE<br>U slučaju da je odgovor DA, opisati prirodu i sadržaj otkrivenih ličnih podataka korisnika  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Aktivnosti koje su preduzete za rješavanje sigurnosnog incidenta                             |  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Subjekti koji su obavješteni o sigurnosnom incidentu   |  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Procijenjeno vrijeme otklanjanja sigurnosnog incidenta                                       |  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Ostale važne informacije   |  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Ime i kontakt podaci lica koje je zaduženo za davanje informacija o incidentu (tel., e-mail) |  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |
| Datum i vrijeme dostave obavještenja   |  |  |                            |                    |       |                  |       |                     |       |                   |       |                          |       |                            |       |        |       |

PRILOG 4:

Kriterijumi za izvještavanje o sigurnosnom incidentu

| Sigurnosni incident  | Minimum krajnjih korisnika/površina teritorije obuhvaćenih sigurnosnim incidentom | Minimalno trajanje sigurnosnog incidenta |
|--|---|--|
| Nemogućnost mreže da prima, ili usmjerava pozive prema brojevima hitnih službi | 1 korisnik  | nezavisno od trajanja                    |
| Onemogućena usluga telefonskih poziva u fiksnoj mreži                          | 1 000 korisnika   | 4 sata                                   |
| Onemogućena usluga telefonskih poziva u fiksnoj mreži                          | 5 000 korisnika   | 1 sat                                    |
| Onemogućena usluga telefonskih poziva i SMS u mobilnoj mreži                   | 46 km <sup>2</sup>  | 4 sata                                   |
| Onemogućena usluga telefonskih poziva i SMS u mobilnoj mreži                   | 138 km <sup>2</sup>   | 1 sat                                    |
| Onemogućena usluga pristupa internetu  | 1 000 korisnika   | 4 sata                                   |
| Onemogućena usluga pristupa internetu  | 5 000 korisnika   | 1 sat                                    |
| Onemogućena usluga distribucije audio vizuelnih sadržaja                       | 1 000 korisnika   | 4 sata                                   |
| Onemogućena usluga distribucije audio vizuelnih sadržaja                       | 5 000 korisnika   | 1 sat                                    |
| Povreda ličnih podataka korisnika  | 1 korisnik  | nezavisno od trajanja                    |

K  
a  
t  
a  
l  
o  
g  
  
P  
r  
o  
p  
i  
s  
a

PRILOG 5:

Izveštaj o sigurnosnom incidentu

|   |  |
|---|--|
| Operator  |  |
| Datum i vrijeme nastanka sigurnosnog incidenta    | 2011   |
| Datum i vrijeme utvrđivanja sigurnosnog incidenta | 5  |
| Način utvrđivanja sigurnosnog incidenta           |  |
| Opis sigurnosnog incidenta                        |  |
| Vrsta usluge koju obuhvata sigurnosni incident    | Fiksna telefonija: <input type="checkbox"/> PSTN <input type="checkbox"/> IMS <input type="checkbox"/> VoIP <input type="checkbox"/> DRUGO _____<br>Fiksni Internet: <input type="checkbox"/> xDSL <input type="checkbox"/> FTTx <input type="checkbox"/> KDS <input type="checkbox"/> DRUGO _____<br>Mobilna telefonija: <input type="checkbox"/> GSM <input type="checkbox"/> UMTS <input type="checkbox"/> LTE <input type="checkbox"/> DRUGO _____<br>Mobilni Internet: <input type="checkbox"/> GPRS/EDGE <input type="checkbox"/> UMTS <input type="checkbox"/> LTE <input type="checkbox"/> DRUGO _____<br>Zemaljska radiodifuzija: <input type="checkbox"/> Zemaljska TV <input type="checkbox"/> Zemaljski radio<br>Distribucija AVM sadržaja: <input type="checkbox"/> KDS <input type="checkbox"/> IPTV <input type="checkbox"/> Satelitski <input type="checkbox"/> MMDS <input type="checkbox"/> DRUGO _____<br>Drugo _____ |

|   | TRAJANJE  | BROJ OBUHVAĆENIH KORISNIKA |
|---|---|----------------------------|
| Vrijeme trajanja sigurnosnog incidenta i broj obuhvaćenih korisnika | Fiksna telefonija: _____<br>Fiksni Internet: _____<br>Mobilna telefonija: _____<br>Mobilni Internet: _____<br>Zemaljska radiodifuzija: _____<br>Distribucija AVM sadržaja: _____<br>Drugo: _____  | _____                      |
| Uticaj na hitne službe  | <input type="checkbox"/> DA <input type="checkbox"/> NE   |                            |
| Uticaj na interkonekciju (u zemlji i inostranstvu)                  | <input type="checkbox"/> DA <input type="checkbox"/> NE   |                            |
| Da li je došlo do povrede ličnih podataka korisnika?                | <input type="checkbox"/> DA <input type="checkbox"/> NE<br>U slučaju da je odgovor DA, opisati prirodu i sadržaj otkrivenih ličnih podataka korisnika   |                            |
| Osnovni uzrok   | <input type="checkbox"/> Sistemske greške<br><input type="checkbox"/> Ljudske greške<br><input type="checkbox"/> Zlonamjerne radnje<br><input type="checkbox"/> Prirodni fenomeni<br><input type="checkbox"/> Greška treće strane<br><input type="checkbox"/> Uzrok nije utvrđen  |                            |
| Početni uzrok   | <input type="checkbox"/> Prekid kabla K<br><input type="checkbox"/> Krađa kabla a<br><input type="checkbox"/> Poplava t<br><input type="checkbox"/> Obilne snježne padavine a<br><input type="checkbox"/> Oluja l<br><input type="checkbox"/> Prekid napajanja p<br><input type="checkbox"/> Električni udar r<br><input type="checkbox"/> Fizički napad o<br><input type="checkbox"/> Kibernetički napad p<br><input type="checkbox"/> Loše održavanje i<br><input type="checkbox"/> Preopterećenje s<br><input type="checkbox"/> Iscrpljene zalihe goriva a<br><input type="checkbox"/> Proceduralna greška 2<br><input type="checkbox"/> Greška hardvera<br><input type="checkbox"/> Programska greška<br><input type="checkbox"/> Ljudska greška<br><input type="checkbox"/> Drugo _____<br><input type="checkbox"/> Uzrok nije utvrđen |                            |

|   |   |
|---|---|
| <p>Sistemi obuhvaćeni početnim uzrokom</p>  | <ul style="list-style-type: none"> <li><input type="checkbox"/> Bazine stanice i upravljački sistemi (npr. BTS, NodeB, RNC)</li> <li><input type="checkbox"/> Mobilni komutacioni sistemi (npr. MSC, VLR, SGSN, GGSN)</li> <li><input type="checkbox"/> Korisnički i lokacioni registri (npr. HLR, HSS, AuC)</li> <li><input type="checkbox"/> Komutacioni sistemi (npr. lokalne centrale, svičevi, DSLAM)</li> <li><input type="checkbox"/> Sistemi prenosa (npr. SDH, WDM)</li> <li><input type="checkbox"/> Interkonekcija</li> <li><input type="checkbox"/> Međunarodna mreža</li> <li><input type="checkbox"/> Sistem napajanja (npr. transformatori, mreža napajanja)</li> <li><input type="checkbox"/> Rezervno napajanje (npr. dizel generatori, baterije)</li> <li><input type="checkbox"/> Sistemi hlađenja</li> <li><input type="checkbox"/> Ulični kabineti</li> <li><input type="checkbox"/> Centar za razmjenu poruka</li> <li><input type="checkbox"/> Adresni serveri (DHCP, DNS)</li> <li><input type="checkbox"/> Backbone mreža</li> <li><input type="checkbox"/> Lokalna mreža (npr. optička, bakarna)</li> <li><input type="checkbox"/> Drugo _____</li> </ul> |
| <p>Rješavanje sigurnosnog incidenta i opis preduzetih mjera (opis aktivnosti koje su preduzete nakon utvrđivanja incidenta za rješavanje incidenta)</p>                                 |   |
| <p>Mjere preduzete nakon otklanjanja sigurnosnog incidenta (opis preduzetih aktivnosti od strane operatora za smanjivanje vjerovatnoće ponavljanja incidenta ili uticaja incidenta)</p> | <p>K<br/>a<br/>t<br/>a<br/>l<br/>o<br/>g</p>  |
| <p>Dugoročne mjere</p>  | <p>P<br/>r<br/>o</p>  |
| <p>Ostale važne informacije</p>   | <p>P<br/>i<br/>s<br/>a</p>  |
| <p>Ime i kontakt podaci lica koje je zaduženo za davanje informacija o incidentu (tel., e-mail)</p>   | <p>©<br/>2<br/>0<br/>1</p>  |
| <p>Datum dostave izvještaja</p>   | <p>5</p>  |