1216.

Na osnovu člana 5 tačka 5 i člana 61 stav 6 Zakona o elektronskim komunikacijama ("Službeni list CG", broj 40/13), Vlada Crne Gore, na sjednici od 30. oktobra 2014. godine, donijela je

UREDBA

O SADRŽINI PLANA MJERA ZA OBEZBJEĐENJE INTEGRITETA JAVNIH ELEKTRONSKIH KOMUNIKACIONIH MREŽA I KORIŠĆENJE ELEKTRONSKIH KOMUNIKACIONIH USLUGA U VANREDNIM SITUACIJAMA

("Službeni list Crne Gore", br. 050/14 od 28.11.2014)

Predmet

Član 1

Ovom uredbom propisuju se mjere koje mora da sadrži plan mjera operatora kojim se obezbjeđuje integritet javne elektronske komunikacione mreže i omogućava korišćenje elektronskih komunikacionih usluga u slučajevima većeg ispada mreže, ratnog i vanrednog stanja, elementarnih nepogoda, kao i drugih vanrednih situacija (u daljem tekstu: Plan mjera).

Vanrednom situacijom, iz stava 1 ovog člana, smatra se stanje izazvano vanrednim okolnostima, prirodnim ili ljudskim faktorom, čime je prouzrokovana neposredna opasnost po život i zdravlje ljudi, imovinu građana ili je značajno ugrožena životna sredina ili kulturno-istorijsko nasljeđe na određenom području.

Sadržina Plana mjera

Član 2

Plan mjera obavezno sadrži mjere kojima se obezbjeđuje:

1) korišćenje javnih elektronskih komunikacionih mreža i usluga za obavještavanje javnosti, za vrijeme vanrednih situacija;

2) poboljšanje pouzdanosti javnih elektronskih komunikacionih mreža i usluga (rezervno napajanje, zalihe rezervne opreme, redundantnost određenih sistema u mreži, odgovarajuća zaštita opreme i sl.) sa utvrđenim rokovima, timovima i kontaktima lica odgovornih za njihovo izvršenje;

3) stalan i nesmetan pristup brojevima hitnih službi, u skladu sa Zakonom o elektronskim komunikacijama, kao i brojevima svih subjekata koji, u skladu zakonom, odlukama i naredbama Vlade djeluju u vanrednim situacijama;

4) primjena u slučaju različitih tipova ispada sistema ili djelova sistema, uključujući i mogućnost izmještanja pojedinih djelova sistema, sa kontaktima lica odgovornih za njihovo izvršenje;

5) neprekidnost rada sistema i upravljanje javnom elektronskom komunikacionom mrežom u vanrednim situacijama sa preciznim planom realizacije i kontaktima lica odgovornih za njihovo izvršenje;

6) saradnja sa drugim operatorima sa ciljem pružanja usluga u vanrednim situacijama, sa kontaktima lica odgovornih za njihovo izvršenje;

7) zajedničko korišćenje kapaciteta i usluga, kao i koordiniranje aktivnosti sa drugim operatorima, sa ciljem obezbjeđivanja prioritetnih usluga i usluga prioritetnim korisničkim grupama, ljudskih i materijalnih resursa, kao i koordinaciju u upravljanju saobraćajem u slučajevima zagušenja u mreži;

8) u okviru zajedničkog sistema digitalnog radija TETRA sistema, za međusobnu komunikaciju svih učesnika koji djeluju u vanrednim situacijama (sistemu zaštite i spašavanja), najmanje jedan S/D i tri simpleksna.

U mjere iz stava 1 ovog člana, obavezno se uključuju i procedure za upravljanje rizicima, sigurnosni zahtjevi za osoblje, sigurnost sistema i prostora, upravljanje postupcima, upravljanje bezbjednosnim incidentima, upravljanje kontinuitetom poslovanja, nadzor i testiranje bezbjednosti.

Mjerama iz stava 1 ovog člana, operatori elektronskih komunikacija su dužni da obezbijede neprekidno pružanje javnih elektronskih komunikacionih usluga putem komunikacionih mreža i stepen sigurnosti, kao odgovor na prijetnje i sigurnosne incidente, i radi ublažavanja njihovog uticaja na rad javne komunikacione mreže, mrežno povezivanje, kao i/ili na javne komunikacione usluge.

Standardi za sprovođenje mjera iz st. 1, 2 i 3 ovog člana i referentne norme za njihovo sprovođenje date su u Prilogu, koji je sastavni dio ove uredbe.

Obaveze operatora fiksne telefonije

Član 3

Operator usluga fiksne telefonije, za vrijeme vanrednih situacija, dužan je da obezbijedi:

1) stalnu i nesmetanu informaciono - komunikacionu infrastrukturu do Operativno komunikacionih centara 112 u Podgorici, Baru i Bijelom Polju (u daljem tekstu: OKC-a 112), pri čemu je za glavnu vrstu konekcije dužan da obezbijedi optički spojni put, a za rezervnu vrstu konekcije radio-relejne (mikro-talasne) linkove;

2) stalnu i nesmetanu informaciono - komunikacionu infrastrukturu do Operativnog centra Generalštaba Vojske Crne Gore (u daljem tekstu: OC GŠ VCG), pri čemu je za glavnu vrstu konekcije dužan da obezbijedi optički spojni put, a za rezervnu vrstu konekcije radio-relejne (mikro talasne) linkove;

3) stalnu i nesmetanu informaciono - komunikacionu infrastrukturu do državnog organa nadležnog za nacionalnu bezbjednost, pri čemu je za glavnu vrstu konekcije dužan da obezbijedi optički spojni put, a za rezervnu vrstu konekcije radio-relejne (mikro-talasne) linkove;

4) stalan i nesmetan informaciono - komunikacioni servis između koordinacionog tima za upravljanje u vanrednim situacijama, OKC-a 112, operativnim centrom Uprave policije, OC GŠ VCG, državnim organom nadležnim za nacionalnu bezbjednost, CIRT timovima (Computer Incident Responce Team) i drugim subjektima uključenim u razrješavanje vanrednih situacija, kao i dovoljan broj priključaka fiksne telefonije, u zavisnosti od vanredne situacije, a u skladu sa odlukom koordinaciog tima, nadležnog za upravljanje u vanrednim situacijama;

5) stalan i nesmetan pristup internetu svim subjektima koji djeluju u vanrednim situacijama.

Obaveze operatora mobilne telefonije

Član 4

Operator usluga mobilne telefonije, za vrijeme vanrednih situacija, dužan je da obezbijedi:

1) stalnu i nesmetanu informaciono-komunikacionu infrastrukturu do OKC-a 112;

2) stalnu i nesmetanu informaciono - komunikacionu infrastrukturu do OC GŠ VCG;

3) stalnu i nesmetanu informaciono - komunikacionu infrastrukturu do državnog organa nadležnog za nacionalnu bezbjednost;

4) stalan i nesmetan informaciono - komunikacioni servis između koordinacionog tima za upravljanje u vanrednim situacijama, OKC-112, OC GŠ VCG, državnog organa nadležnog za nacionalnu bezbijednost, CIRT timovima (Computer Incident Responce Team) i drugim subjektima koji djeluju u vanrednim situacijama, kao i dovoljan broj mobilnih telefona i/ili SIM kartica, u zavisnosti od nastale situacije, a u skladu sa odlukom koordinacionog tima nadležnog za upravljanje u vanrednim situacijama;

5) stalan i nesmetan pristup internetu svim institucijama koje djeluju u vanrednim situacijama.

Obaveze operatora zajedničkog sistema digitalnog radija - TETRA

Član 5

Operatori zajedničkog sistema digitalnog radija - TETRA, za vrijeme vanrednih situacija, dužni su da:

1) obezbijede neprekidnost sistema radio veza u vanrednim situacijama;

2) stave na raspolaganje ručne radio-uređaje (terminale) za institucije koje djeluju u vanrednim situacijama.

Način komunikacije

Član 6

Planovi aktivnosti, odluke i međusobne komunikacije koje se odvijaju za vrijeme vanrednih situacija između državnih organa, organa državne uprave, organa lokalne samouprave i lokalne uprave, operatora elektronskih komunikacija i drugih nadležnih subjekata, moraju biti sačinjeni u pisanoj formi.

Pružanje usluga bez naknade

Član 7

Korišćenje opreme i usluga koje su operatori elektronskih komunikacija stavili na raspolaganje subjektima koji djeluju u vanrednim situacijama, za vrijeme vanrednih situacija, ne tarifira se.

Rok za donošenje plana mjera

Član 8

Operatori elektronskih komunikacija donose plan mjera najkasnije do novembra tekuće, za narednu godinu.

Stupanje na snagu

Član 9

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

Broj: 08-2556/4

Podgorica, 30. oktobra 2014. godine

Vlada Crne Gore

Predsjednik,

Milo Đukanović, s.r.

PRILOG

PRILOG

STANDARDI I NORME ZA SPROVOĐENJE PLANA MJERA

Minimalne mjere bezbjednosti	Referentne norme	Opis
Procedure za upravljanje rizicima	MEST ISO/IEC 27001/2 i MEST ISO/IEC27005	MEST ISO/IEC 27005 opisuje procedure za upravljanje rizicima. MEST ISO/IEC27002 u poglavlju 5. opisuje politiku informacione sigurnosti, procedure za upravljanje rizicima i kontrolu trećih strana (dobavljače usluga (hardvera i softvera)), kao što su bezbjednosni zahtjevi i postupak nabavke za nadogradnju ili kupovinu informacionog sistema.
Bezbjednosni zahtjevi za osoblje	MEST ISO/IEC 27001/2	MEST ISO/IEC 27001/2 upoglavlju 8. opisuje bezbjednosne provjere osoblja, sigurnosne uloge i odgovornosti, bezbjednosno znanje i osposobljavanje te promjene osoblja.
Bezbjednost sistema i prostora	MEST ISO/IEC 27001/2	MESTISO/lEC 27001 u poglavlju 9.opisuje fizičku bezbjednost prostora, IT opreme i kontrolu okoline
Upravljanje postupcima	MEST ISO/IEC 27001/2	MEST ISO/IEC 27001 u poglavlju 10. opisuje operativne procedure, uloge, klasifikaciju, kontrolu pristupa i kontrolu promjene
Upravljanje bezbjednosnim Incidentima	MESTISO/lEC 27001/2	MEST ISO/IEC 27002 u poglavlju 13. opisuje upravljanje bezbjednosnim incidentima
Upravljanje kontinuitetom poslovanja	MEST ISO/IEC 22301	MEST ISO/IEC 22301 opisuje upravljanje kontinuitetom poslovanja
Nadzor i testiranje bezbjednosti	MEST ISO/IEC 27001/2	Nadzor je opisan u poglavlju 10. MESTISO/IEC27001/2, dok su testiranje sigurnosti, usklađenost nadzora i obavje-štavanje opisani u poglavlju 15. MEST ISO/IEC 27001/2.