`Në bazë të nenit 68 paragrafët (2) dhe (3) të Ligjit për ndjekje të komunikimeve ("Gazeta zyrtare e RMV-së nr. 71/2018 dhe 108/2019), drejtori i Agjencisë Teknike-Operative Shkup miratoi

**RREGULLORE**

për masat dhe standardet për siguri informative të cilat operatorët e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike publike duhet t'i respektojnë detyrimisht në lidhje me detyrimet për zbatim të masave për ndjekje të komunikimeve

## I. DISPOZITAT E PËRGJITHSHME

### Objekt i rregullimit
### Neni 1

Me këtë Rregullore përcaktohen masat dhe standardet për siguri informative të sistemeve informative të cilat janë të detyruar t'i zbatojnë operatorët e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike publike në lidhje me detyrimet e tyre për zbatim të masave për ndjekje të komunikimeve në pajtim me Ligjin për ndjekje të komunikimeve.

### Detyrimet e operatorëve

### Neni 2

Operatorët e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike janë të detyruar t'i zbatojnë masat dhe standardet për siguri informative, në pajtim me dispozitat e kësaj Rregullore.

### Qëllimi i masave dhe standardeve për siguri informative

### Neni 3

Me këtë Rregullore vendosen masat dhe standardet e sigurisë me të cilat do të sigurohet konfidencialitet, integritet dhe disponueshmëri e informatave.

## II. MASAT DHE STANDARDET PËR SIGURI INFORMATIVE

### Raportet e operatorëve për kontrolle të kryera të brendshme të rregullta
### Neni 4

(1) Operatorët kryejnë kontrolle të brendshme të rregullta për funksionimin, efektet dhe dobësitë në sigurinë e sistemeve informative dhe për atë përgatisin raporte me shkrim.
(2) Raportet nga paragrafi (1) vihen jepen për kontroll me kërkesë të Komisionit për Mbikëqyrje Profesionale të Punës së Operatorëve (në tekstin e mëtutjeshëm Komisioni).
(3) Operatorët janë të detyruar që t'ua japin për kontroll anëtarëve të Komisionit procesverbalet nga mbikëqyrjet e kryera të rregullta nga Drejtoria për Mbrojtje të të

Dhënave Personale, Agjencia për Komunikime Elektronike dhe Drejtoria për siguri të Informatave të Klasifikuara.

**Caktimi i personit përgjegjës për zbatimin e masave dhe standardeve për siguri informative**

**Neni 5**

Operatorët e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike janë të detyruar të caktojnë person përgjegjës për zbatimin e masave dhe standardeve të sigurisë informative.

**Detyrimet e personit përgjegjës për zbatimin e masave dhe standardeve të sigurisë informative**

**Neni 6**

Personi përgjegjës për zbatimin e masave dhe standardeve të sigurisë informative:

- Kryen koordinim të të gjitha aktiviteteve të sigurisë lidhur me vendosjen dhe ruajtjen e sigurisë informative;
- Menaxhon me vlerësimet periodike të rreziqeve për sigurinë informative;
- Kryen vlerësim të rregullt të rreziqeve dhe përditësimeve të planeve për përballje me rreziqet prioritare;
- E përditëson evidencën e ligjeve dhe rreziqeve potenciale;
- E koordinon realizimin e kontrolleve të sigurisë dhe e mbikëqyr efikasitetin e tyre;
- Propozon politikë dhe pjesëmarrje për arritje të sistemit të sigurt informativ;
- Merr pjesë në përgatitjen e akteve të brendshme, politikave teknike dhe plotësuese komplementare me të cilat sigurohet zbatimi i politikave dhe udhëzimeve për sistem të sigurt informativ;
- E mbikëqyr zbatimin e akteve të brendshme për siguri të sistemit informativ;
- Kryen koordinim të brendshëm dhe hetim të ngjarjeve që e kanë rrezikuar sigurinë e sistemit informativ, përfshirë edhe bashkëpunimin me organet e jashtme dhe institucionet tjera;
- Propozon masa për tejkalimin e pasojave dhe parandalimin e incidenteve të ngjashme;
- Bashkëpunon me personat përgjegjës të sistemeve informative në ATO;
- Parashtron kërkesë për ngritje të procedurës për përcaktimin e përgjegjësisë për shkelje të rregullave të sigurisë së sistemit informativ.

**Standardet dhe rregullat e sigurisë së sistemeve informative**

**Neni 7**

Standardet dhe rregullat e sigurisë së sistemeve informative përfshijnë:

- Kritere minimale dhe masa të sigurisë që duhet t'i përmbushin sistemet informative;
- Udhëzime të përgjithshme minimale për mbrojtjen e informacioneve për ndryshime të paautorizuara të qëllimshme dhe të paqëllimshme, shkatërrim se zbulim;
- Shfrytëzim të standardeve të sigurisë nga seria MKS ISO/IEC 27000 në sistemet informative;

- Kontroll të rregullt i sigurisë së sistemeve informative;
- Vlerësim të rregullt të rreziqeve lidhur me sigurinë e sistemeve informative, prioritetin e tyre, si dhe masat për përballje me rreziqet në rast të paraqitjes së tyre;
- Menaxhim me incidente lidhur me sigurinë informative;
- Kompetencë dhe përgjegjësi për futje, menaxhim dhe mbikëqyrje të sigurimit të sistemeve informative.

**Masat e sigurisë informative të sistemeve informative**
**Neni 8**

Masat për siguri informative të sistemeve informative që janë të detyruar t'i zbatojnë operatorët e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike në lidhje me detyrimet e tyre për zbatimin e masave për ndjekje të komunikimeve në pajtim me Ligjin për ndjekje të komunikimeve janë:

1. Shërbimet e pashfrytëzuara dhe protokollet doemos duhet të çaktivizohen;
2. Disponueshmëria e serviseve doemos duhet të kufizohet;
3. Softueri i pashfrytëzuar doemos duhet të çinstalohet (nuk lejohet të instalohet softuer i sistemit që nuk është i nevojshëm për punë, mirëmbajtje ose funksion të sistemit);
4. Funksionet e pashfrytëzuara të softuerit dhe harduerit operativ doemos duhet të çaktivizohen;
5. Komponentët softuerikë dhe harduerikë të cilët e kanë arritur fundin e afatit të përdorimit ose nuk kanë kontratë për mbështetje nuk guxojnë të përdoren;
6. Dobësitë e paraqitura në softuerin dhe harduerin e sistemit doemos duhet të jenë të fiksuara ose të mbrojtura nga keqpërdorimi;
7. Të dhënat nga nevoja për mbrojtje doemos duhet të jenë të mbrojtura nga shikimi i paautorizuar dhe manipulimi gjatë transferimit dhe ruajtjes;
8. Informata të ndjeshme (informata lidhur me ndjekjen elektronike të komunikimeve) nuk guxojnë të përfshihen në skedat ose porositë që janë të disponueshme për shfrytëzuesit e paautorizuar;
9. Sistemet doemos duhet të jenë të qëndrueshëm kundër situatave me stërngarkim (doemos duhet të shmanget pjesërisht ose plotësisht dëmtimi i sistemeve, gjatë a.q. sulmeve DoS);
10. Sistemi doemos duhet të jetë i qëndrueshëm kundër futjes së papritur të të dhënave;
11. Pa autentifikim dhe autorizim i suksesshëm nuk guxon të lejohet qasje në funksione dhe informata të sistemeve;
12. Doemos duhet të shfrytëzohen llogari të përdoruesit që mundësojnë identifikim të qartë të përdoruesit;
13. Llogaritë e përdoruesit doemos duhet të jenë të mbrojtur nga përdorimi i paautorizuar me së paku një atribut për autentifikim;
14. Llogaritë e përdoruesit me të drejta të gjera doemos duhet të jenë të mbrojtura me dy atribute për autentifikim;
15. Llogaritë e para e paradefinuara dhe të pashfrytëzuara doemos duhet të fshihen ose të pamundësohen;

16. Atributet e paradefinuara për autentifikim doemos duhet të fshihen ose pamundësohen;
17. Privilegjet për llogaritë e përdoruesit dhe aplikacionet doemos duhet të reduktohen në minimum i nevojshëm për detyrat që duhet t'i kryejnë;
18. Sistemi doemos duhet të lidhet me sistemin qendror për administrimin e përdoruesve;
19. Sesionet doemos duhet të mbrohen nga kidnapimi (përdorimi i metodave të kriptografisë, masat mbrojtëse në nivel të rrjetit, transportit, në nivel aplikativ);
20. Sistemi doemos duhet të ketë funksion që lejon që përdoruesi që është lidhur të shkëputet në cilëndo kohë;
21. Sistemi doemos duhet të ketë funksion që lejon që sesioni aktiv të ndërpritet automatikisht pas një kohe të caktuar të çaktivizimit;
22. Nëse përdoret fjalëkalimi i si atribut për kontroll, ajo duhet doemos të ketë së paku tetë karaktere dhe të përmbajë tre nga kategoritë vijuese: shkronja të mëdha, shkronja të vogla, numra dhe shenja speciale;
23. Nëse përdoret fjalëkalimi si atribut për kontroll, doemos të zbatohen masa për mbrojtje nga sulmet e dhunshme që e pengojnë goditjen e fjalëkalimit;
24. Nëse përdoret fjalëkalimi si atribut për kontroll, doemos duhet të jetë i fshehur kur paraqitet në ekran;
25. Të dhënat për t'u lidhur relevante për sigurinë doemos duhet të dërgohen në sistemin e jashtëm (në skedat përkatëse) drejtpërdrejt pas krijimit të tyre;
26. Të sigurohet bekap i elementeve të rrjetit me funksionalitetin LI;
27. Sistemet doemos duhet të lidhen në sistemin redundant të karikimit me energji elektrike;
28. Sistemet doemos duhet të jenë të mbrojtur nga fatkeqësitë elementare dhe ndikimet e jashtme.

## Mirëmbajtja e sistemit informativ

### Neni 9

Personat fizikë ose juridikë që kryejnë mirëmbajtje të sistemit informativ të operatorëve duhet t'i zbatojnë rregullat për siguri informative të përcaktuara me këtë Rregullore.

### Siguria fizike e sistemeve

### Neni 10

(1) Sistemet që janë të involvuar në procesin e ndjekjes së komunikimeve te operatorët duhet të jenë fizikisht të vendosura në hapësirat e sigurta.
(2) Qasje fizike në hapësirën në të cilën janë vendosur sistemet mund të kenë vetëm personat me autorizime të veçanta.
(3) Nëse nevojitet qasje të personit tjetër në hapësirat ku janë vendosur sistemet, atëherë ai person duhet të shoqërohet dhe mbikëqyret nga personi nga paragrafi (2) i këtij neni.
(4) Hapësira në të cilën janë vendosur serverët mbrohet nga rreziqet në mjedisin përmes zbatimit të masave dhe kontrolleve me të cilat ulet rreziku nga kërcënimet potenciale,

përfshirë vjedhje, zjarr, shpërthime, tym, ujë, pluhur, vibracione, ndikime kimike, pengesa në furnizimin me energji elektrike dhe rrezatim magnetik.

## III. MËNYRA E MENAXHIMIT ME INCIDENTET

### Menaxhimi me incidente
### Neni 11

Operatorët duhet të formojnë ekip për menaxhim me incidente lidhur me sigurinë informative dhe të vendosin procedura për ndjekje dhe menaxhim me incidentet e sigurisë.

### Rregullat për menaxhim me incidentet e sigurisë
### Neni 12

Ekipi për menaxhim me incidentet e sigurisë përgatit Rregulla për menaxhim me incidentet e sigurisë të cilat duhet t'i përmbajnë elementet në vijim:

- Lista e funksioneve të rëndësishme të identifikuara të sistemit dhe prioritetet për përtëritje të funksionaliteteve të sistemit;
- Lista e resurseve të identifikuara të cilat janë të domosdoshme për përmbushje të funksioneve të rëndësishme kritike;
- Lista e incidenteve të mundshme me gjasa për paraqitjen e tyre, duke dalë nga vlerësimet e rrezikut;
- Strategjitë e përpunuara për përtëritje të funksionalitetit të sistemit;
- Masat e definuara për realizim të strategjive.

### Evidentimi dhe ruajtja e dokumentacionit për sistemet informatike
### Neni 13

Personi përgjegjës për zbatimin e masave dhe standardeve për siguri informative duhet ta evidentojë dhe ta ruajë dokumentacionin e plotë për sisteme informative të operatorëve dhe për të gjitha ndryshimet e tyre.

## IV. DISPOZITAT PËRFUNDIMTARE
### Neni 14

Kjo Rregullore hyn në fuqi në ditën e miratimit të saj.

27.8.2019
Shkup

Drejtor
**Zoran Angellovski**