Врз основа на член 8 став (3), а во врска со член 4 став (1) точки 1), 2) и 8), член 4 ставови (2) и (3), член 8 ставови (1), (2), (4) и (5), член 11 став (1) точка 2) и член 16 од Законот за безбедност на мрежни и информациски системи („Службен весник на Република Северна Македонија" бр. 135/25), директорот на Агенцијата за електронски комуникации, на 14.07. 2026 година, ја донесе следната

**ПРЕДЛОГ - МЕТОДОЛОГИЈА**

**ЗА ПРОЦЕНКА НА РИЗИК ЗАРАДИ ИДЕНТИФИКУВАЊЕ НА СУШТИНСКИ И ВАЖНИ СУБЈЕКТИ ОД НАДЛЕЖНОСТ НА АГЕНЦИЈАТА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ ПРЕКУ НАЦИОНАЛНИОТ ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ — MKD-CIRT**

## I. ОПШТИ ОДРЕДБИ

### Предмет
### Член 1

(1) Со оваа Методологија се пропишуваат критериумите и начинот на проценка на ризик заради идентификување и класификување на:

1) други субјекти кои, врз основа на проценка на ризик, се утврдуваат како суштински субјекти согласно член 8 став (1) точка 8) од Законот за безбедност на мрежни и информациски системи (во натамошниот текст: Законот);

2) други субјекти кои, врз основа на проценка на ризик, се утврдуваат како важни субјекти согласно член 8 став (2) точка 2) од Законот.

(2) Методологијата претставува аналитичка и постапковна рамка преку која Агенцијата за електронски комуникации (во натамошниот текст: Агенцијата), во функција на надлежен орган за безбедност на мрежни и информациски системи преку Националниот центар за одговор на компјутерски инциденти MKD-CIRT (во натамошниот текст: MKD-CIRT), ги класифицира субјектите од своја надлежност како суштински, односно како важни субјекти, и го предлага нивното вклучување во деталните листи од член 7 став (1) од Законот.

(3) Методологијата не се применува за субјектите кои согласно Законот непосредно имаат статус на суштински, односно на важни субјекти, освен како помошна аналитичка алатка за приоритизација на надзорот, ажурирање на податоците и подготовка и одржување на електронската листа на субјекти од надлежност на Агенцијата.

### Опфат на примена
### Член 2

(1) Оваа Методологија се применува за субјектите од надлежност на Агенцијата преку MKD-CIRT, согласно член 11 став (1) точка 2) од Законот, и тоа:

1) субјектите од член 4 став (1) точки 1), 2) и 8) од Законот;

2) субјектите од член 4 став (2) од Законот;

3) субјектите од член 4 став (3) од Законот.

(2) Кога за определена област од член 4 став (2) или став (3) од Законот, со посебен закон е назначен или воспоставен друг надлежен орган согласно член 11 став (2) од Законот, оваа Методологија се применува без задирање во надлежноста на тој орган. Агенцијата остварува соработка и размена на податоци со другите надлежни органи заради избегнување преклопување и обезбедување на единствен пристап во класификацијата.

**Дефиниции**
**Член 3**

За потребите на оваа Методологија, поодделните изрази го имаат следното значење:

1) „Законот" е Законот за безбедност на мрежни и информациски системи („Службен весник на Република Северна Македонија" бр. 135/25);

2) „Министерството" е Министерството за дигитална трансформација;

3) „проценка на ризик" е аналитичка постапка спроведена од Агенцијата преку MKD-CIRT за определување на ризикот по безбедноста на мрежните и информациските системи на субјект, заради утврдување на неговата класификација согласно член 1 од оваа Методологија;

4) „субјект" е физичко или правно лице од опфатот на оваа Методологија согласно член 2;

5) „критериум" е ризик-фактор пропишан со оваа Методологија преку кој се оценува ризикот по безбедноста на мрежните и информациските системи поврзан со определен субјект;

6) „значителен ризик" е такво ниво на ризик чие настапување може да предизвика значителни нарушувања во функционирањето на услугата, во работењето на субјектот или во меѓусебно зависните области, а во смисла на оваа Методологија се изразува со четири или со пет поени по конкретен критериум;

7) другите изрази употребени во оваа Методологија го имаат значењето утврдено во член 3 од Законот.

**Општи принципи на проценката на ризик**
**Член 4**

(1) Проценката на ризик согласно оваа Методологија се заснова на следните принципи:

1) објективност — оценувањето се врши врз основа на проверливи, документирани и недвосмислено утврдени факти;

2) пропорционалност — обемот на проценката и побараните податоци се во сразмер со целта на класификацијата и со природата на услугата;

3) транспарентност — критериумите, начинот на бодувањето и образложението на одлуката се јасно утврдени и достапни до субјектот, во рамките на прописите за класифицирани информации и за заштита на безбедносно чувствителни податоци;

4) недискриминација — за сите субјекти со споредливи карактеристики се применуваат истите критериуми и истиот начин на бодување;

5) континуирано следење — класификацијата се преиспитува редовно и се ажурира кога ќе настанат релевантни промени.

(2) Проценката на ризикот се врши преку следните критериуми (ризик-фактори):

1) единствен давател на услуги;

2) влијание врз јавната безбедност, јавната заштита или јавното здравје;

3) системски ризик и прекугранично влијание;

4) специфично национално значење.

(3) Секој критериум од став (2) на овој член се оценува со определен број поени, при што најниските број поени изнесува 1, а највисокиот број поени изнесува 5. Поголемиот број поени укажува на повисоко ниво на критичност, поголема зависност од услугата, поголемо потенцијално влијание и повисок ризик по безбедноста на мрежните и информациските системи.

(4) Критериумите од став (2) на овој член произлегуваат од член 4 став (3) точки 5), 6), 7) и 8) од Законот и се применуваат кумулативно, при што конечната класификација се определува согласно член 9 од оваа Методологија.

## II. КРИТЕРИУМИ ЗА ПРОЦЕНКА НА РИЗИК

### Единствен давател на услуги
### Член 5

(1) Преку критериумот „единствен давател на услуги" се оценува уникатноста на субјектот при обезбедувањето услуга од значење во национален, секторски или регионален контекст. Целта е да се утврди дали постојат алтернативни даватели кои навремено и без значителни последици би можеле да ја одржат услугата во случај на прекин, нарушување, компромитација или деградација на услугата на субјектот.

(2) Бодувањето по овој критериум се врши на следниот начин:

1) 1—2 поени — субјектот работи на конкурентен пазар или во средина со повеќе одржливи алтернативи; нарушувањето би било управливо и би имало минимално општествено, економско или секторско влијание поради можноста услугата да биде обезбедена од други даватели;

2) 3 поени — субјектот е еден од неколкуте даватели на услугата; прекинот во неговото работење може да предизвика значителни проблеми, привремени локализирани прекини или отежнато обезбедување на услугата до воспоставување алтернатива;

3) 4 поени — субјектот е еден од многу ограничен број даватели и е критичен за поголем дел од државата, секторот, подсекторот или за значителна група корисници; прекинот би предизвикал големо, но не и целосно нарушување на услугата;

4) 5 поени — субјектот е единствениот или практично незаменливиот давател на услуга која е суштинска за критична општествена, економска, јавна, дигитална или

инфраструктурна активност, при што секое нарушување може да предизвика непосредни и широко распространети последици.

**Влијание врз јавната безбедност, јавната заштита или јавното здравје**
**Член 6**

(1) Преку критериумот „влијание врз јавната безбедност, јавната заштита или јавното здравје" се оценуваат непосредните и посредните последици од прекин, нарушување, компромитација или деградација на услугата врз безбедноста, здравјето, животот и благосостојбата на граѓаните, како и врз способноста на надлежните институции да обезбедат јавни функции и услуги.

(2) Бодувањето по овој критериум се врши на следниот начин:

1) 1—2 поени — нарушувањето на услугата би предизвикало минимални или ограничени последици, без непосредна закана за јавната безбедност, јавната заштита или јавното здравје;

2) 3 поени — прекинот или нарушувањето би имало забележливо влијание и би барало координиран, но не и обемен јавен или институционален одговор;

3) 4 поени — нарушувањето би претставувало значителна закана за јавната безбедност, јавната заштита или јавното здравје, би можело да влијае на голема популација или на значаен број институции и би барало обемен јавен или институционален одговор;

4) 5 поени — нарушувањето би претставувало непосредна, широко распространета и директна закана за човечки живот, за јавната безбедност, за јавната заштита или за јавното здравје.

**Системски ризик и прекугранично влијание**
**Член 7**

(1) Преку критериумот „системски ризик и прекугранично влијание" се оценува можноста нарушувањето на услугата на субјектот да предизвика системски нарушувања, каскадни последици или последици што се протегаат надвор од националните граници.

(2) Проценката по овој критериум ги зема предвид: поврзаноста на услугата на субјектот со други субјекти, сектори, подсектори, јавни институции и критични услуги; зависноста на дигиталната инфраструктура и ланците на снабдување од услугата на субјектот; и можноста инцидентот да се прошири на национално или меѓународно ниво.

(3) Бодувањето по овој критериум се врши на следниот начин:

1) 1—2 поени — услугата на субјектот е во голема мера изолирана; нарушувањето би било ограничено и не би предизвикало системски ризик ниту прекугранично влијание;

2) 3 поени — прекинот може да предизвика умерен системски ризик во непосредниот сектор или ограничен прекуграничен ефект врз специфична меѓузависна услуга;

3) 4 поени — нарушувањето би предизвикало значителен системски ризик, широко распространети нарушувања во сопствениот сектор, умерено до високо влијание врз други клучни национални сектори или јасно утврдено прекугранично влијание;

4) 5 поени — нарушувањето би предизвикало значителен системски ризик со широко распространети каскадни последици во повеќе критични сектори, на национално или меѓународно ниво.

**Специфично национално значење**

**Член 8**

(1) Преку критериумот „специфично национално значење" се оценува уникатната, стратешката или незаменливата улога на субјектот во определен сектор, подсектор, тип услуга или во национален контекст, особено кога значењето на субјектот произлегува не само од тоа дали е единствен давател на услугата, туку и од неговата посебна важност за функционирањето на определена област, дигитална услуга, критична инфраструктура, јавна функција или меѓусебно зависни области во Републиката.

(2) Бодувањето по овој критериум се врши на следниот начин:

1) 1—2 поени — субјектот има ограничена улога во својот сектор, а нарушувањето би имало занемарливо или ниско влијание врз вкупната функционалност на секторот;

2) 3 поени — субјектот е значаен локален или регионален давател; неговото нарушување би имало забележливо влијание врз определен дел од територијата, но не би ја нарушило функционалноста на секторот на национално ниво;

3) 4 поени — субјектот е клучен давател чии услуги се суштински за голем дел од секторот, подсекторот или за значителна група корисници, при што нарушувањето сериозно би ја погодило функционалноста на секторот на национално ниво;

4) 5 поени — субјектот е основен за својот сектор или има посебна важност на национално или регионално ниво за конкретна услуга или за други меѓузависни сектори, како што се услугите поврзани со националната размена на интернет-сообраќај, врвните национални интернет домени, доверливите услуги, јавните електронски комуникациски мрежи, ДНС, услугите за компјутерска обработка во облак, податочните центри, управуваните ИКТ услуги или други услуги од високо национално значење.

## III. КЛАСИФИКАЦИЈА И ПРАГОВИ

### Класификациска матрица и прагови
### Член 9

(1) Конечната класификација на субјектот се определува според највисокиот резултат добиен по кој било од критериумите од член 4 став (2) од оваа Методологија (метод на најкритичен критериум).

(2) Класификацијата се врши на следниот начин:

1) субјект кој по најмалку еден критериум добил 5 поени се класифицира како суштински субјект;

2) субјект кој по најмалку еден критериум добил 4 поени, а по ниту еден критериум не добил 5 поени, се класифицира како важен субјект;

3) субјект кој по сите критериуми добил најмногу 3 поени, не се класифицира како суштински ниту како важен субјект врз основа на оваа Методологија, освен ако со закон не е определено поинаку.

(3) Кога субјектот добил 4 поени по два или повеќе критериуми и кога постојат стручни и објективно проверливи индикации за зголемено влијание врз безбедноста на мрежните и информациските системи, MKD-CIRT може во стручното мислење да предложи класификација на субјектот како суштински субјект, со детално образложение.

(4) Кога постојат посебни околности кои не се целосно опфатени со бодувањето, како што се специфични технолошки зависности, концентрација на критични функции, новонастанати закани или други оправдани причини, MKD-CIRT во стручното мислење ги утврдува тие околности и предлага соодветна класификација во рамките на Законот.

(5) Регулаторните импликации од класификацијата (мерките за управување со сајбер безбедносни ризици, обврските за пријавување и режимот на надзор) се утврдени со Законот и со подзаконските акти донесени врз основа на Законот.

(6) Прегледот на класификацијата според највисокиот резултат е даден во следната табела:

| Резултат | Класификација | Регулаторни импликации |
|---|---|---|
| 5 поени | Суштински субјект | Обврски за мерки за управување со сајбер безбедносни ризици, обврски за пријавување значајни сајбер безбедносни инциденти и значајни сајбер закани, како и режим на надзор согласно Законот. |
| 4 поени | Важен субјект | Обврски за мерки за управување со сајбер безбедносни ризици и обврски за пријавување, при што надзорот се врши екс пост согласно член 51 од Законот. |
| 1—3 поени | Без класификација по оваа Методологија | Не се класифицира како суштински ниту како важен субјект врз основа на оваа Методологија, освен ако со закон не е определено поинаку. |

## IV. ПОСТАПКА ЗА ПРОЦЕНКА НА РИЗИК

### Постапка
### Член 10

(1) Постапката за проценка на ризик ги опфаќа следните чекори:

1) почетна идентификација на субјектот и проверка дали припаѓа во опфатот од член 2 на оваа Методологија;

2) прибирање и проверка на податоците потребни за проценката;

3) оценување на субјектот по секој од критериумите од член 4 став (2) на оваа Методологија;

4) изработка на стручно мислење со предлог за класификација;

5) донесување одлука за класификација од директорот на Агенцијата;

6) евидентирање на субјектот во електронската листа од член 8 став (4) од Законот и доставување на податоците до Министерството заради утврдување и ажурирање на деталните листи од член 7 став (1) од Законот;

7) континуирано следење и периодично преиспитување.

(2) Проценката на ризик ја спроведува MKD-CIRT.

(3) Заради објективност, MKD-CIRT во проценката може да ангажира експерти од соодветни области, при што се применуваат правилата за избегнување на судир на интереси и за заштита на доверливи податоци.

### Извори на податоци
### Член 11

(1) Заради спроведување на проценката, Агенцијата преку MKD-CIRT може да собира потребни податоци и информации преку:

1) директни барања до субјектот — Агенцијата има право да побара од субјектот информации, податоци и документи потребни за проценката, при што субјектот е должен да ги достави побараните податоци на потребното ниво на детали во рок од 20 дена од денот на приемот на барањето, освен ако со барањето не е определен пократок рок поради итност;

2) надзорни активности — податоци утврдени преку стручен надзор, проверки, ревизии, технички анализи или други активности согласно Законот;

3) извештаи за инциденти — информации од претходни сајбер безбедносни инциденти, значајни сајбер закани, избегнати инциденти, ранливости и од задолжителни и доброволни известувања;

4) јавно достапни извори — податоци од јавни регистри, годишни извештаи, секторски публикации, интернет-страници, постапки за јавни набавки, регулаторни објави и други јавно достапни извори;

5) информации од други надлежни органи — податоци доставени од Министерството, од секторски регулатори, од органите надлежни за критична инфраструктура и од други органи и институции, во рамките на Законот и на посебните прописи.

(2) При прибирањето и обработката на податоците се применуваат прописите за заштита на личните податоци и за класифицирани информации.

**Стручно мислење и одлука за класификација**
**Член 12**

(1) По завршување на проценката, MKD-CIRT подготвува стручно мислење што содржи:

1) идентификациски податоци за субјектот;

2) опис на услугите кои ги дава субјектот, а кои се релевантни за проценката;

3) бодување по секој од критериумите со образложение;

4) применет метод на конечна класификација согласно член 9 од оваа Методологија;

5) предлог за класификација (суштински субјект, важен субјект или невклучување во електронската листа);

6) посебни околности и стручни забелешки, доколку постојат.

(2) Врз основа на стручното мислење, директорот на Агенцијата донесува одлука за класификација на субјектот.

(3) Одлуката од став (2) на овој член се доставува до субјектот на кој се однесува, освен кога со закон, со прописите за класифицирани информации или поради заштита на безбедносно чувствителни информации, доставувањето е ограничено или исклучено.

(4) Субјектот има право на правна заштита против одлуката од став (2) на овој член, во согласност со Законот за општата управна постапка и со Законот за управните спорови.

**Самопријавување од субјектите**
**Член 13**

(1) Субјект кој не е вклучен во деталната листа на суштински субјекти, односно во деталната листа на важни субјекти, а ги исполнува условите да биде на тие листи, е должен до Агенцијата како надлежен орган да достави известување согласно член 8 став (5) од Законот.

(2) По приемот на известувањето од став (1) на овој член, Агенцијата преку MKD-CIRT ја применува оваа Методологија заради утврдување на класификацијата на субјектот.

(3) Кога субјектот не достави известување согласно став (1) на овој член, а Агенцијата ќе утврди дека ги исполнува условите за класификација, се применуваат прекршочните одредби согласно Законот.

## V. ПРЕИСПИТУВАЊЕ И СОРАБОТКА

### Преиспитување и ажурирање
### Член 14

(1) Класификацијата на субјектите се преиспитува редовно, а најмалку еднаш на две години, или пред истекот на тој рок кога ќе настанат релевантни промени, и тоа особено:

1) суштински промени во опсегот, природата или критичноста на услугите кои ги дава субјектот;

2) суштински промени во структурата или работењето на субјектот, вклучувајќи статусни промени;

3) промени во секторот, подсекторот или во релевантната ИКТ инфраструктура;

4) појава на нови сајбер закани или ранливости со значително влијание;

5) измени и дополнувања на Законот, на ЕУ и меѓународните стандарди и на другите релевантни прописи;

6) барање на самиот субјект со оправдани причини.

(2) Преиспитувањето се спроведува преку постапката од член 10 на оваа Методологија.

(3) Резултатите од преиспитувањето се внесуваат во електронската листа од член 8 став (4) од Законот и се доставуваат до Министерството.

### Доверливост на податоците
### Член 15

(1) Податоците содржани во електронската листа од член 8 став (4) од Законот, како и податоците добиени и обработени во постапката за проценка на ризик, се сметаат за класифицирани информации со соодветен степен на тајност, согласно член 7 став (10) од Законот и согласно Законот за класифицирани информации.

(2) Лицата ангажирани во проценката на ризик согласно оваа Методологија се должни да ја почитуваат тајноста и доверливоста на податоците на кои имаат пристап, и оваа обврска трае и по престанокот на нивниот ангажман.

### Соработка со други надлежни органи
### Член 16

(1) Заради единствен пристап и избегнување на преклопување, Агенцијата преку MKD-CIRT соработува со Министерството и со другите надлежни органи од член 11 од Законот при подготовката и ажурирањето на деталните листи од член 7 став (1) од Законот.

(2) Агенцијата преку MKD-CIRT соработува со органот на државната управа надлежен за управување со критична инфраструктура заради усогласување на класификацијата со податоците за сопствениците и операторите на критична инфраструктура.

(3) Соработката се одвива согласно Законот и врз основа на склучени меморандуми, односно протоколи за соработка.

## VI. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

### Прва проценка на ризик
### Член 17

(1) Првата проценка на ризик согласно оваа Методологија се спроведува заради утврдување на електронската листа од член 8 став (4) од Законот, а најдоцна до истекот на рокот од член 58 став (2) од Законот.

(2) До завршувањето на првата проценка, Агенцијата може да ги применува критериумите од оваа Методологија како помошна аналитичка рамка во рамките на подготвителните активности.

### Влегување во сила
### Член 18

(1) Методологија за проценка на ризик заради идентификување на суштински и важни субјекти од надлежност на Агенцијата за електронски комуникации преку Националниот центар за одговор на компјутерски инциденти MKD-CIRT започува да се применува со денот на објавувањето во „Службен весник на Република Северна Македонија".

По влегувањето во сила, оваа Методологија ќе биде објавена и на веб страната на Агенцијата за електронски комуникации.

Бр. 0101-1513/13
14.04. 2026 година
Скопје

**Директор**
на Агенцијата за електронски комуникации
Nusret Haliti

Изготвил:
Раководител на MKD-CIRT
Sevdali Selmani