Врз основа на член 33 став (12) од Законот за безбедност на мрежни и информациски системи („Службен весник на Република Северна Македонија“ бр. 135/2025), во врска со член 11 став (1) точка 2), член 20 став (1), член 33 ставови (1)–(11) и член 61 став (2) од истиот закон, по претходно добиена согласност од Министерството за дигитална трансформација бр. 14.07. од 2026. година, Директорот на Агенцијата за електронски комуникации донесува

ПРЕДЛОГ - МЕТОДОЛОГИЈА
за поблиските критериуми и праговите за определување на обични и значајни сајбер безбедносни инциденти по области за субјектите од надлежност на Агенцијата за електронски комуникации преку Националниот центар за одговор на компјутерски инциденти — MKD-CIRT

Напомена: Оваа методологија има правно дејство по добивање на претходна согласност од Министерството за дигитална трансформација. Методологијата се ажурира најмалку еднаш годишно, согласно член 33 став (12) од Законот.

I. ОПШТИ ОДРЕДБИ

Член 1
(Предмет)

(1) Со оваа методологија се утврдуваат поблиските критериуми и праговите за определување дали еден сајбер безбедносен инцидент се класифицира како обичен или како значаен сајбер безбедносен инцидент, за областите и субјектите од надлежност на Агенцијата за електронски комуникации преку Националниот центар за одговор на компјутерски инциденти — MKD-CIRT.

(2) Методологијата содржи заедничка рамка применлива на сите области од надлежност на Агенцијата, како и посебни секторски прилози со конкретни прагови и критериуми за секоја област поединечно.

(3) Секторските прилози се составен дел на оваа методологија и претставуваат методологии по области во смисла на член 33 став (12) од Законот.

Член 2
(Цел)

1) да обезбеди јасна, објективна и применлива основа за класификација на инцидентите како обични или значајни;
2) да обезбеди правна сигурност за суштинските и важните субјекти при исполнување на обврските за известување;
3) да обезбеди навремено активирање на обврските за пријавување и известување од член 33 од Законот;
4) да овозможи споредливост на податоците во оперативната евиденција, Националниот регистар на сајбер инциденти и извештаите до Министерството;
5) да ја поддржи ситуационата свесност, раното предупредување, координацијата и управувањето со сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи;

6) да обезбеди усогласување со релевантните европски и меѓународни норми, добри практики и технички спецификации, со примена во рамките на националниот правен систем.

Член 3
(Опфат и применливост)

(1) Оваа методологија се применува за субјектите од надлежност на Агенцијата за електронски комуникации преку MKD-CIRT, и тоа:

1) Собранието на Република Северна Македонија;
2) самостојните државни органи и регулаторните тела основани од и одговорни пред Собранието;
3) судовите;
4) субјектите од областите со висока критичност од член 4 став (2) од Законот, во рамките на примената на Законот;
5) субјектите од другите критични области од член 4 став (3) од Законот; и
6) други субјекти кои со закон или врз основа на проценка на ризик се утврдуваат како суштински или важни субјекти од надлежност на Агенцијата.

(2) Методологијата не се применува на субјектите од извршната власт за кои надлежен е MKD-GOV-CSIRT, освен во случаи на меѓусебна зависност, инцидент со голем опфат, сајбер безбедносна криза или потреба од координација помеѓу тимовите.

(3) За областите од член 4 став (2) точки 8) до 16) од Законот, за кои примената е одложена согласно член 61 став (2) од Законот, секторските прилози се подготвуваат и се активираат во согласност со динамиката утврдена со Законот и со процесот на пристапување на Република Северна Македонија во Европската унија.

Член 4
(Начела)

1) законитост — класификацијата се врши само врз основа на Законот и оваа методологија;
2) пропорционалност — прагот за значајност се толкува според природата, големината, критичноста и ризичниот профил на субјектот;
3) конзервативна проценка — кога постои основано сомневање дека може да настане сериозно влијание, инцидентот привремено се третира како значаен до утврдување на фактите;
4) докажливост — секоја класификација се документира со факти, проценки, технички податоци или образложение;
5) споредливост — се користат унифицирани димензии и секторски прагови за да се овозможи национална статистика и анализа;
6) минимизација на податоци — се обработуваат само податоци неопходни за класификација, известување и справување со инцидентот;
7) заштита на доверливост — информациите се третираат согласно TLP ознаките, прописите за класифицирани информации, деловна тајна и заштита на лични податоци.

II. ПОИМИ И ДЕФИНИЦИИ

Член 5
(Поими)

Изразите употребени во оваа методологија го имаат значењето определено во Законот. За целите на оваа методологија дополнително се применуваат следните поими:

1) „обичен сајбер безбедносен инцидент" е инцидент кој не ги исполнува критериумите и праговите за значаен сајбер безбедносен инцидент, но може да биде предмет на евидентирање, техничка анализа и оперативна поддршка;
2) „праг на значајност" е квантитативна или квалитативна граница над која инцидентот се класифицира како значаен;
3) „квантитативен праг" е мерлив праг изразен преку траење, број на засегнати корисници, обем на засегнати услуги, финансиска штета, број на засегнати субјекти, технички параметри или други мерливи показатели;
4) „квалитативен критериум" е околност која сама по себе укажува на значајност на инцидентот, независно од тоа дали се достигнати мерливите прагови;
5) „критична услуга" е услуга чиј прекин, нарушување, компромитација или деградација може да предизвика сериозно влијание врз функционирањето на субјектот, други субјекти, корисници, јавната безбедност, јавната заштита, јавното здравје, економијата, дигиталната инфраструктура или довербата во институциите;
6) „момент на дознавање" е моментот кога субјектот, преку одговорно лице, офицер за сајбер безбедност, дежурна служба, SOC, надворешен давател или друг овластен канал, дознал или разумно морал да дознае дека постои инцидент;
7) „избегнат инцидент со значајно потенцијално влијание" е избегнат инцидент кој, доколку не бил спречен, би ги исполнил критериумите за значаен сајбер безбедносен инцидент;
8) „значајна сајбер закана" е закана која, според техничките карактеристики, веродостојноста и изложеноста на субјектот, може да доведе до значаен сајбер безбедносен инцидент.

III. ЗАЕДНИЧКА РАМКА ЗА КЛАСИФИКАЦИЈА

Член 6
(Двостепен модел)

(1) Класификацијата на инцидентот се врши преку двостепен модел:

1) проверка на секторските и заедничките квантитативни прагови; и
2) проверка на квалитативните критериуми за значајност.

(2) Инцидентот се класифицира како значаен ако е исполнет најмалку еден секторски или заеднички квантитативен праг или најмалку еден квалитативен критериум.

(3) Инцидентот за кој не е исполнет ниту еден квантитативен праг и ниту еден квалитативен критериум се класифицира како обичен.

(4) Класификацијата се врши веднаш по првичното дознавање и се преиспитува при секоја значајна промена на фактите, опфатот, последиците или техничките сознанија.

Член 7
(Димензии на влијание)

Димензија	Опис
Д1 — Оперативно влијание	траење, степен на недостапност, деградација, нарушување на критични процеси или услуги
Д2 — Засегнати корисници и субјекти	број и значење на засегнати физички лица, правни лица, институции, корисници или зависни субјекти
Д3 — Финансиско и економско влијание	директна и индиректна финансиска штета, измама, договорни последици, трошоци за обновување
Д4 — Јавна безбедност, јавна заштита и здравје	ризик за живот, здравје, безбедност, јавен ред, услуги од јавен интерес или итни служби
Д5 — Доверливост, интегритет и достапност на податоци	компромитација, неовластена измена, губење, недостапност или откривање на податоци
Д6 — Географски и прекуграничен опфат	локално, регионално, национално или прекугранично влијание
Д7 — Каскадно и системско влијание	пренесено влијание врз други субјекти, сектори, добавувачи или критични услуги

Член 8
(Заеднички квалитативни критериуми)

Независно од квантитативните прагови, инцидентот се класифицира како значаен ако е исполнет најмалку еден од следните критериуми:

1) инцидентот предизвикал или може да предизвика сериозно нарушување на услугите на суштински или важен субјект;
2) инцидентот влијаел или може да влијае врз други физички или правни лица со значителна материјална или нематеријална штета;
3) постои потврдено или основано сомневање за прекугранично влијание;
4) инцидентот влијае врз критична инфраструктура, критична услуга, јавна безбедност, јавна заштита, јавно здравје, демократски процес, судска постапка или законодавна функција;
5) инцидентот се однесува на компромитација на привилегирани сметки, администраторски пристап, криптографски клучеви, доверливи услуги, DNS, регистар на домени или инфраструктура за електронска идентификација;
6) инцидентот е дел од координирана кампања, supply-chain напад, ransomware напад, DDoS напад со значаен капацитет или активна експлоатација на критична ранливост;
7) инцидентот создава каскадно влијание врз најмалку еден друг суштински субјект или врз повеќе важни субјекти;
8) инцидентот бара активирање на план за континуитет на работењето, план за обновување по катастрофа, кризен план или ескалација кон национален координативен механизам;

9) инцидентот предизвикува или може да предизвика сериозна повреда на доверливоста, интегритетот или достапноста на лични, службени, деловно чувствителни или класифицирани информации;

10) инцидентот е од таква природа што непријавувањето би можело да ја попречи ситуационата свесност, раното предупредување или координацијата на национално ниво.

Член 9

(Заеднички квантитативни прагови)

(1) Освен ако со секторски прилог не е определен поспецифичен или построг праг, се применуваат следните заеднички прагови:

Димензија	Суштински субјект	Важен субјект
Прекин на критична услуга	1 час или повеќе	4 часа или повеќе
Прекин на друга важна услуга	4 часа или повеќе	24 часа или повеќе
Засегнати корисници	5% од корисничката база или 25.000 корисници	10% од корисничката база или 100.000 корисници
Финансиски загуби	500.000 евра во денарска противвредност или 1% од годишниот приход	1.500.000 евра во денарска противвредност или 3% од годишниот приход
Компромитација на лични податоци	100 субјекти на лични податоци или било кој обем на чувствителни лични податоци	1.000 субјекти на лични податоци или 100 субјекти со чувствителни податоци
Влијание врз други субјекти	5 субјекти со пренесено влијание	25 субјекти со пренесено влијание

(2) Ако секторскиот прилог утврдува посебен праг, се применува секторскиот праг.

(3) Ако се достигнати два или повеќе прагови, инцидентот се третира како значаен со повисок степен на сериозност и се ескалира без одлагање.

Член 10

(Категории на сериозност на значајните инциденти)

Категорија	Услов	Оперативна последица
S1 — значаен	исполнет е најмалку еден праг или еден квалитативен критериум	редовно постапување како значаен инцидент и известување согласно член 33
S2 — многу сериозен	исполнети се два или повеќе прагови/критериуми или постои секторско/национално влијание	итна ескалација во MKD-CIRT и засилен мониторинг

S3 — критичен	инцидент со потенцијал за голем опфат или сајбер безбедносна криза	итна ескалација до раководството на АЕК, Министерството и, кога е применливо, националните координативни механизми

Категориите S1, S2 и S3 не ја менуваат обврската за пријавување; тие служат за внатрешна ескалација, приоритизација на ресурсите и координација.

IV. ПОСТАПКА ЗА КЛАСИФИКАЦИЈА

Член 11
(Чекори на класификацијата)

1) утврдување на моментот на дознавање за инцидентот;
2) идентификација на засегнатиот субјект, сектор, услуга и критичност на услугата;
3) прибирање на достапни факти, технички показатели и информации за влијанието;
4) проверка на применливиот секторски прилог;
5) проверка на заедничките и секторските квантитативни прагови;
6) проверка на квалитативните критериуми;
7) утврдување на класификацијата: обичен или значаен инцидент;
8) утврдување на категоријата на сериозност S1, S2 или S3, кога инцидентот е значаен;
9) документирање на класификацијата и активирање на обврските за известување.

Член 12
(Конзервативен пристап)

(1) Ако во моментот на првичното дознавање не се достапни доволно информации, но постои основано сомневање дека инцидентот може да биде значаен, субјектот го третира инцидентот како значаен и ги активира обврските за пријавување.

(2) Ако последователно се утврди дека инцидентот не ги исполнува критериумите за значаен, тоа се документира во известувањето или завршната анализа.

(3) Конзервативниот пристап не претставува замена за анализа; тој служи само за избегнување на задоцнето пријавување кога фактите се непотполни.

Член 13
(Документирање)

Класификацијата се документира во евиденцијата на субјектот, во оперативната евиденција на MKD-CIRT и, кога е применливо, во Националниот регистар на сајбер инциденти. Записот содржи најмалку:

1) идентификатор на инцидентот;
2) датум и време на дознавање и класификација;

3) лице или функција што ја извршило класификацијата;

4) применет секторски прилог;

5) достигнати квантитативни прагови;

6) исполнети квалитативни критериуми;

7) класификација: обичен или значаен;

8) категорија S1, S2 или S3, кога е применливо;

9) образложение и докази;

10) датум и време на известување до MKD-CIRT.

V. ВРСКА СО ОБВРСКИТЕ ЗА ПРИЈАВУВАЊЕ

Член 14
(Активирање на роковите)

(1) Класификацијата како значаен инцидент ги активира обврските за пријавување согласно член 33 од Законот.

1) иницијално известување — веднаш, а најдоцна во рок од три часа од моментот на дознавање;

2) рано предупредување — во рок од 24 часа;

3) известување за инцидентот — во рок од 72 часа;

4) привремени известувања — на барање на MKD-CIRT;

5) завршно известување — во рок од еден месец;

6) извештаи за напредок и завршен извештај — кога инцидентот продолжува и по завршното известување.

(2) Роковите течат од моментот на дознавање, а не од моментот на завршена внатрешна анализа или потврда од трета страна.

Член 15
(Промена на класификација)

(1) Ако инцидент првично класифициран како обичен подоцна ги исполни критериумите за значаен, субјектот без одлагање доставува известување до MKD-CIRT.

(2) Промената на класификацијата се документира со наведување на новите факти, моментот на дознавање и причините за рекласификација.

(3) Ако инцидентот првично е пријавен како значаен, а подоцна се утврди дека е обичен, субјектот доставува образложение во завршното известување или во последователна корекција на записот.

Член 16
(Значајни сајбер закани и избегнати инциденти)

(1) Оваа методологија соодветно се применува и за проценка дали значајна сајбер закана или избегнат инцидент би можеле да имаат значајно потенцијално влијание.

(2) Кога значајна сајбер закана или избегнат инцидент укажува на можност за значаен инцидент, субјектот го известува MKD-CIRT заради рано предупредување, ситуациона свесност и спречување на каскадни ефекти.

VI. СЕКТОРСКИ ПРИЛОЗИ

Секторските прилози го утврдуваат минималниот праг за значајност по области. Кога инцидентот опфаќа повеќе сектори, се применува најстрогиот релевантен праг.

Член 17
(Прилог А — ЕНЕРГЕТИКА: опфат и критични услуги)

(1) Овој прилог се применува на: Субјекти кои обезбедуваат услуги во секторот енергетика, вклучувајќи електрична енергија, нафта, гас, топлинска енергија и оператори на енергетски пазари, во рамките на надлежноста на АЕК/MKD-CIRT.

(2) Критични услуги за целите на овој прилог се:

1) управување со пренос и дистрибуција на електрична енергија
2) одржување на стабилност на електроенергетски систем
3) снабдување со електрична енергија, гас, нафта и топлинска енергија
4) SCADA/EMS/DMS и други OT системи

Член 18
(Прилог А — специфични прагови)

Димензија / услуга	Праг за значајност
Загубена електрична енергија	50 MWh во 24 часа како резултат на сајбер инцидент
Засегнати потрошувачи	10.000 крајни потрошувачи без снабдување повеќе од 60 минути или 1.000 повеќе од 4 часа
SCADA/OT влијание	секоја неовластена команда, промена на параметар или компромитација на SCADA/EMS/DMS
Стабилност	секој сајбер настан што бара емергентни процедури за стабилност на системот
Критични потрошувачи	секое влијание врз снабдување на болници, итни служби, водоснабдување или телекомуникации

Покрај наведените прагови, се применуваат и заедничките квалитативни критериуми од член 8 на оваа методологија.

Член 19

(Прилог Б — ТРАНСПОРТ: опфат и критични услуги)

(1) Овој прилог се применува на: Субјекти во воздушен, железнички, друмски и јавен транспорт, вклучувајќи системи за управување со сообраќај, резервација, наплата и критични транспортни платформи.

(2) Критични услуги за целите на овој прилог се:

1) управување со воздушен сообраќај
2) железничка сигнализација и управување
3) системи за патарини и интелигентни транспортни системи
4) јавен превоз и системи за билети

Член 20

(Прилог Б — специфични прагови)

Димензија / услуга	**Праг за значајност**
ATM/ATC услуги	секој прекин или нарушување, без оглед на траењето
Летови	5 или повеќе откажани/одложени летови во 6 часа поради сајбер инцидент
Железничка сигнализација	прекин повеќе од 30 минути или било кое влијание врз ETCS/GSM-R/CTC
Патници	1.000 истовремено засегнати или 10.000 во 24 часа
Наплатни системи	прекин на електронска наплата повеќе од 4 часа

Покрај наведените прагови, се применуваат и заедничките квалитативни критериуми од член 8 на оваа методологија.

Член 21

(Прилог В — БАНКАРСТВО: опфат и критични услуги)

(1) Овој прилог се применува на: Кредитни институции и други субјекти од банкарскиот сектор во рамките на надлежноста на АЕК/MKD-CIRT, со координација со Народната банка кога е применливо.

(2) Критични услуги за целите на овој прилог се:

1) core banking
2) платен промет
3) електронско и мобилно банкарство
4) картични системи, ATM/POS и SWIFT

Член 22

(Прилог В — специфични прагови)

Димензија / услуга	Праг за значајност
Core banking	прекин повеќе од 30 минути во работно време
Платен промет	прекин повеќе од 30 минути
Е-банкарство/мобилно банкарство	прекин или значајна деградација 1 час или повеќе
ATM/POS	прекин на 25% или повеќе од мрежата 1 час или повеќе
Финансиска штета	250.000 евра во денарска противвредност или повеќе
SWIFT	секој успешен или сериозно подозреван неавторизиран обид

Покрај наведените прагови, се применуваат и заедничките квалитативни критериуми од член 8 на оваа методологија.

Член 23

(Прилог Г — ИНФРАСТРУКТУРА НА ФИНАНСИСКИТЕ ПАЗАРИ: опфат и критични услуги)

(1) Овој прилог се применува на: Оператори на места за тргување, централни депозитари, системи за клиринг и порамнување и други овластени учесници во инфраструктурата на финансиските пазари.

(2) Критични услуги за целите на овој прилог се:

1) тргување
2) порамнување и клиринг
3) пазарни податоци
4) налози, трансакции и позиции

Член 24

(Прилог Г — специфични прагови)

Димензија / услуга	Праг за значајност
Прекин на тргување	прекин во работно време повеќе од 30 минути
Прекин на порамнување/клиринг	прекин повеќе од 1 час
Пазарни податоци	нецелосни или недостапни податоци 30 минути или повеќе
Финансиска штета	500.000 евра во денарска противвредност или повеќе
Компромитација на тргувачки податоци	секоја компромитација на доверливост или интегритет

Покрај наведените прагови, се применуваат и заедничките квалитативни критериуми од член 8 на оваа методологија.

Член 25

(Прилог Д — ЗДРАВСТВО: опфат и критични услуги)

(1) Овој прилог се применува на: Болници, клиники, референтни лаборатории, субјекти за истражување и развој на лекови, производители на основни фармацевтски производи и медицински помагала.

(2) Критични услуги за целите на овој прилог се:

1) ургентни и болнички услуги
2) HIS/EMR системи
3) лабораториски системи
4) поврзани медицински уреди
5) критичен ланец на снабдување со лекови

Член 26

(Прилог Д — специфични прагови)

Димензија / услуга	**Праг за значајност**
Неодложни медицински услуги	секое нарушување на ургентен прием, операциона сала, интензивна нега или итна помош
HIS/EMR	прекин 1 час или повеќе во работно време
LIS	прекин што влијае на дијагностика 2 часа или повеќе
Медицински уреди	секоја компромитација или нарушување на поврзани уреди
Здравствени податоци	компромитација на здравствени податоци на 100 или повеќе пациенти
Лекови/вакцини	прекин на критичен ланец на снабдување повеќе од 24 часа

Покрај наведените прагови, се применуваат и заедничките квалитативни критериуми од член 8 на оваа методологија.

Член 27

(Прилог Ѓ — ДИГИТАЛНА ИНФРАСТРУКТУРА: опфат и критични услуги)

(1) Овој прилог се применува на: IXP, DNS, регистар на домени .mk и .мкд, облак, податочни центри, CDN, доверливи услуги и јавни електронски комуникациски мрежи и услуги.

(2) Критични услуги за целите на овој прилог се:

1) DNS и TLD услуги
2) јавни електронски комуникациски мрежи и услуги
3) облак и податочни центри

4) доверливи услуги

5) CDN и интерконекција

Член 28

(Прилог Ѓ — специфични прагови)

Димензија / услуга	Праг за значајност
DNS	прекин 30 минути или повеќе или влијание врз 5% од барањата
Јавна комуникациска услуга	100.000 корисници 30 минути или 10.000 корисници 2 часа
Податочен центар	прекин на критичен сегмент 30 минути или повеќе
Облак	прекин што влијае на 100 клиенти или 1.000 крајни корисници
TLD регистар	секое влијание врз регистрирање, обновување или резолуција
Доверлива услуга	секоја компромитација на инфраструктура за квалификувани сертификати или електронски потписи
BGP/интерконекција	неавторизирана рута, route leak/hijack или прекин 1 час или повеќе

Покрај наведените прагови, се применуваат и заедничките квалитативни критериуми од член 8 на оваа методологија.

Член 29

(Прилог Е — УПРАВУВАЊЕ СО ИКТ-УСЛУГИ: опфат и критични услуги)

(1) Овој прилог се применува на: Даватели на управувани услуги и управувани безбедносни услуги за други правни лица.

(2) Критични услуги за целите на овој прилог се:

1) managed services
2) managed security services
3) RMM платформи
4) SOC/SIEM услуги
5) централизирани конзоли

Член 30

(Прилог Е — специфични прагови)

Димензија / услуга	Праг за значајност
Засегнати клиенти	5 или повеќе клиенти со компромитиран систем или услуга
Прекин на управувани услуги	10 или повеќе клиенти 1 час или повеќе

RMM/централна конзола	секоја компромитација на алатка за оддалечено управување
Суштински клиент	секое влијание врз клиент кој е суштински субјект
MSSP/SOC	секое нарушување на капацитетот за откривање или одговор

Покрај наведените прагови, се применуваат и заедничките квалитативни критериуми од член 8 на оваа методологија.

Член 31
(Прилог Ж — ИНСТИТУЦИОНАЛЕН СЕКТОР ОД НАДЛЕЖНОСТ НА АЕК/MKD-CIRT: опфат и критични услуги)

(1) Овој прилог се применува на: Собранието, самостојните државни органи и регулаторните тела основани од и одговорни пред Собранието и судовите.

(2) Критични услуги за целите на овој прилог се:

1) основни институционални функции
2) судски и законодавни процеси
3) електронски услуги кон граѓани
4) службени, регистарски и судски податоци

Член 32
(Прилог Ж — специфични прагови)

Димензија / услуга	**Праг за значајност**
Основни функции	прекин или значајно нарушување 2 часа или повеќе во работно време
Електронски услуги кон граѓани	прекин 4 часа или повеќе
Службени/судски податоци	секоја компромитација на интегритет или доверливост
Е-пошта	прекин 4 часа или повеќе
Акредитиви	компромитација на 10 или повеќе службени корисници или било кој привилегиран корисник
Седница/расправа	секое нарушување на работа на седница на Собранието или јавна судска расправа

Покрај наведените прагови, се применуваат и заедничките квалитативни критериуми од член 8 на оваа методологија.

Член 33

(Прилог 3 — СУБЈЕКТИ ОД ЧЛЕН 4 СТАВ (3) ОД ЗАКОНОТ: опфат и критични услуги)

(1) Овој прилог се применува на: Субјекти од другите критични области, вклучувајќи даватели/оператори на јавни електронски комуникациски мрежи и услуги, доверливи услуги, регистар на врвни домени, DNS и други субјекти со посебно влијание.

(2) Критични услуги за целите на овој прилог се:

1) јавни електронски комуникациски мрежи и услуги
2) доверливи услуги
3) врвни домени
4) DNS услуги
5) единствени даватели на услуги од суштинско значење

Член 34

(Прилог 3 — специфични прагови)

Димензија / услуга	**Праг за значајност**
Јавни електронски комуникации	се применуваат праговите од Прилог Ѓ
Квалификуван сертификат	секој потврден или сериозно подозревана компромитација на приватен клуч
Издавање/отповикување сертификати	прекин 30 минути или повеќе
CRL/OCSP	секое нарушување на дистрибуција или одговори
Регистар .mk/.мкд	секое нарушување на DNS зони или интегритет на регистарот без оглед на траење

Покрај наведените прагови, се применуваат и заедничките квалитативни критериуми од член 8 на оваа методологија.

VII. СОГЛАСНОСТ, АЖУРИРАЊЕ И ТРАНСПАРЕНТНОСТ

Член 35

(Претходна согласност на Министерството)

(1) Оваа методологија има правно дејство по претходна писмена согласност од Министерството за дигитална трансформација.

(2) Барањето за согласност го доставува Директорот на Агенцијата за електронски комуникации, со приложен текст на методологијата и образложение.

(3) Секоја измена и дополнување на оваа методологија подлежи на претходна согласност од Министерството.

Член 36
(Годишно ажурирање)

(1) Методологијата се ажурира најмалку еднаш годишно.

(2) Годишното преиспитување ги опфаќа:

1) оперативната статистика за обични и значајни инциденти;
2) проверка на доследноста на класификациите;
3) потреба од прилагодување на праговите;
4) научени поуки од сериозни и критични инциденти;
5) усогласување со промени во националното и европското законодавство, техничките стандарди и релевантните добри практики.

(3) Ажурираната методологија се доставува до Министерството заради согласност најдоцна до 28 февруари за тековната година, освен ако поради итни причини не е потребно вонредно ажурирање.

Член 37
(Вонредно ажурирање)

1) значајна промена во националниот или секторскиот закановен пејзаж;
2) нов тип инциденти или закани кои не се соодветно опфатени;
3) значајна промена на Законот или на поврзаните подзаконски акти;
4) утврдена недоследност во практичната примена;
5) потреба од усогласување со нови европски или меѓународни технички спецификации.

Член 38
(Објавување)

(1) Методологијата и нејзините измени се објавуваат на интернет страницата на Агенцијата за електронски комуникации, освен делови кои содржат информации со ограничен пристап согласно закон.

(2) Секоја верзија се означува со број на верзија, датум на добивање согласност и датум на примена.

(3) За класификација на инцидент се применува верзијата на методологијата која е во сила на денот на дознавање за инцидентот.

VIII. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 39
(Примена врз тековни инциденти)

(1) Оваа методологија се применува на инциденти за кои моментот на дознавање настапил по денот на нејзиното влегување во сила.

(2) Тековните инциденти започнати пред денот на влегување во сила продолжуваат да се класифицираат според критериумите што биле применувани во моментот на дознавање,

освен ако примената на оваа методологија е поповолна за навремено известување и координација.

Член 40
(Поддршка во примената)

MKD-CIRT обезбедува стручна поддршка за примената на оваа методологија преку:

1) објаснувачки насоки и работни шаблони;
2) обуки за офицери за сајбер безбедност и лица одговорни за класификација;
3) консултативна поддршка во сомнителни случаи;
4) публикување на анонимизирани примери и најчести грешки во класификацијата.

Член 41
(Влегување во сила)

(1) Методологија за поблиските критериуми и праговите за определување на обични и значајни сајбер безбедносни инциденти по области за субјектите 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. 0101-1513/15

14.07. 2026 година

Скопје

Директор

на Агенцијата за електронски комуникации

Nusret Haliti

Изготвил:

Раководител на MKD-CIRT
Sevdali Selmani