Врз основа на член 16 став (6) од Законот за безбедност на мрежни и информациски системи („Службен весник на Република Северна Македонија“ бр. 135/2025), директорот на Агенцијата за електронски комуникации донесе

ПРАВИЛНИК

за формата, содржината и начинот на водење на Националниот регистар на сајбер инциденти

I. ОПШТИ ОДРЕДБИ

Член 1
(Предмет)

Со овој правилник се уредуваат формата, содржината и начинот на водење на Националниот регистар на сајбер инциденти (во натамошниот текст: Регистарот), начинот на внесување, обработка, ажурирање, чување, користење, заштита и пристап до податоците во Регистарот, како и начинот на доставување податоци од тимовите за одговор на компјутерски инциденти.

Член 2
(Цели на Регистарот)

(1) Регистарот претставува централен национален регистар на податоци за сајбер инциденти кои се доставуваат до Националниот центар за одговор на компјутерски инциденти — MKD-CIRT, согласно Законот за безбедност на мрежни и информациски системи (во натамошниот текст: Законот).

(2) Регистарот се води заради:

1) обезбедување централизирана, точна, навремена и структурирана слика за сајбер инцидентите на национално ниво;
2) поддршка на ситуациона свесност, рано предупредување, координација и стратешко одлучување;
3) обезбедување основа за полугодишните и годишните извештаи кои MKD-CIRT ги доставува до Министерството за дигитална трансформација согласно член 16 став (3) од Законот;
4) обезбедување податоци за подготовка на Годишниот извештај за состојбите во сајбер безбедноста согласно член 34 од Законот;
5) поддршка на координираното справување со сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи;
6) овозможување пристап на органите од областа на безбедноста, одбраната и спроведувањето на законот, во обем неопходен за извршување на нивните законски надлежности;
7) анализа на трендови, типови инциденти, засегнати сектори, закани, ранливости, кампањи и заканувачи, согласно закон и применливите правила за доверливост и заштита на податоци.

Член 3

(Применливост)

(1) Во Регистарот се внесуваат податоци за сајбер инциденти за кои, согласно Законот, тимовите за одговор на компјутерски инциденти доставуваат извештај до MKD-CIRT.

(2) Сите тимови за одговор на компјутерски инциденти, согласно член 16 став (2) од Законот, се должни веднаш, а најдоцна во рок од пет дена од денот на настанувањето на инцидентот, да достават извештај до MKD-CIRT за настанатиот инцидент.

(3) Регистарот не ги заменува оперативните евиденции што ги водат тимовите за одговор на компјутерски инциденти, надлежните органи или субјектите согласно други подзаконски акти, туку претставува национална консолидирана евиденција за сајбер инциденти.

Член 4

(Одговорност за водење)

(1) Регистарот го води MKD-CIRT како посебна организациона единица во рамките на Агенцијата за електронски комуникации, согласно член 16 став (1) точка 10) од Законот.

(2) Раководителот на MKD-CIRT е оперативно одговорен за водењето на Регистарот, за координација на внесот и ажурирањето на податоците и за обезбедување на нивната комплетност, точност, навременост и безбедност.

(3) Директорот на Агенцијата за електронски комуникации обезбедува услови, човечки ресурси, технички капацитети и буџетски средства потребни за воспоставување, одржување и развој на Регистарот.

II. ФОРМА И СТРУКТУРА НА РЕГИСТАРОТ

Член 5

(Форма на Регистарот)

(1) Регистарот се води во електронска форма, во наменски информациски систем за водење на Националниот регистар на сајбер инциденти (во натамошниот текст: Систем на Регистарот).

(2) Системот на Регистарот се воспоставува на начин кој овозможува техничка и оперативна поврзаност со единствениот портал за сајбер безбедност што го воспоставува Министерството за дигитална трансформација согласно член 15 ставови (5) и (6) од Законот.

(3) Системот на Регистарот може да обезбеди внес и размена на податоци преку:

1) безбеден веб-интерфејс за овластени корисници;
2) автоматизиран технички интерфејс (API), доколку е воспоставена техничка интеграција;
3) увоз на структурирани податоци или документи во стандардизирани формати;
4) безбедна електронска комуникација, како привремено или резервно решение;
5) други технички начини кои обезбедуваат автентичност, интегритет, доверливост и следливост на доставените податоци.

(4) Форматите, техничките спецификации, начинот на автентикација, авторизација и размена на податоци се уредуваат со техничко-организациско упатство на MKD-CIRT, усогласено со Министерството за дигитална трансформација кога се однесува на единствениот портал за сајбер безбедност.

Член 6

(Структура на записот)

(1) Секој запис во Регистарот се идентификува со единствен национален идентификатор на инцидентот.

(2) Националниот идентификатор се формира во формат: „NRSI-YYYY-NNNNNNN", каде што „YYYY" ја означува годината на првичниот внес, а „NNNNNNN" е последователен седумцифрен број.

(3) Записот во Регистарот се состои од:

1) задолжителни, односно минимални полиња, без кои записот не може да се смета за уредно внесен; и
2) дополнителни, односно условни полиња, кои се пополнуваат кога податоците се применливи, достапни и неопходни за опис, анализа, координација или известување за инцидентот.

Член 7

(Задолжителни полиња)

Записот во Регистарот најмалку ги содржи следните податоци:

1) национален идентификатор на инцидентот;
2) изворен тим за одговор на компјутерски инциденти и негов локален идентификатор на инцидентот, доколку постои;
3) датум и време на настанување на инцидентот, односно датум и време на утврдување кога точното време на настанување не е познато;
4) датум и време на пријавување или идентификување на инцидентот од изворниот тим;
5) датум и време на доставување на податоците до MKD-CIRT;
6) категорија на инцидент според националната таксономија или применливата шема за класификација;
7) ниво на сериозност или приоритет;
8) статус на постапување;
9) статус на значајност: значаен, обичен, избегнат инцидент или непознато;
10) област, подобласт и вид субјект, доколку е применливо;
11) тип на засегнат субјект: суштински субјект, важен субјект, институција од јавниот сектор, друг субјект или непознато;
12) географски опфат и, доколку е применливо, засегнати држави;
13) информација дали постои сомневање за злонамерно или незаконско дејствување;
14) ознака за распределба на информации, вклучително TLP ознака кога се применува;
15) датум, време и идентитет на овластеното лице кое го извршило последниот внес или ажурирање.

Член 8

(Дополнителни и условни полиња)

Кога се применливи, достапни и неопходни, записот во Регистарот може да содржи и:

1) индикатори за загрозеност, во дефангирана, хеширана, псевдонимизирана или друга безбедна форма;

2) информации за користени тактики, техники и процедури, вклучително референци кон MITRE ATT&CK или друга релевантна рамка;

3) поврзаност со познати закани, кампањи, ранливости или заканувачи, со наведување на ниво на доверба;

4) оценка на влијанието врз доверливост, интегритет и достапност;

5) број или проценка на бројот на засегнати субјекти, корисници или физички лица;

6) оперативно, финансиско, репутациско, регулаторно или друго влијание;

7) информација дали инцидентот е поврзан со можност за повреда на лични податоци;

8) статус на известување до други надлежни органи, засегнати држави или меѓународни партнери, кога е применливо;

9) временска линија на клучни активности во справувањето со инцидентот;

10) преземени и препорачани мерки за ублажување, закрепнување и превенција;

11) научени поуки и препораки;

12) информација за евентуално упатување до органите надлежни за гонење на сторители на кривични дела;

13) врски кон поврзани записи, кога инцидентот е дел од серија, кампања или поширок настан.

Член 9

(Минимизација на лични податоци)

(1) Личните податоци во Регистарот се обработуваат само до степен што е неопходен за целите на Законот, водењето на Регистарот, описот, анализата, координацијата и решавањето на инцидентот.

(2) Согласно член 33 став (11) од Законот, секој личен податок во извештаите за значаен сајбер безбедносен инцидент се ограничува на она што е строго неопходно за опис и решавање на инцидентот.

(3) Личните податоци кои не се неопходни за водењето на Регистарот се анонимизираат, псевдонимизираат или се издвојуваат во посебен заштитен сегмент со ограничен пристап.

(4) Идентитетот на физички лица — пријавители, корисници, жртви или други засегнати лица — не се внесува во основниот запис на Регистарот, освен ако тоа е неопходно и дозволено согласно закон.

III. НАЧИН НА ДОСТАВУВАЊЕ, ВНЕС И АЖУРИРАЊЕ

Член 10

(Рокови за доставување и внес)

(1) Тимовите за одговор на компјутерски инциденти ги доставуваат извештаите за настанатите инциденти до MKD-CIRT веднаш, а најдоцна во рок од пет дена од денот на настанување на инцидентот, согласно член 16 став (2) од Законот.

(2) Кога инцидентот е значаен, со голем опфат, со прекугранично влијание или може да влијае врз јавната безбедност, јавната заштита, јавното здравје, критична инфраструктура или повеќе субјекти, изворниот тим доставува податоци до MKD-CIRT без непотребно одлагање, во рамките на роковите и постапките утврдени со Законот и правилниците за пријавување и постапување по инциденти.

(3) MKD-CIRT го внесува или верификува записот во Регистарот по приемот на податоците, без непотребно одлагање, водејќи сметка за точноста, комплетноста и безбедноста на податоците.

Член 11

(Валидација и тријажа)

(1) Овластено лице во MKD-CIRT врши валидација и тријажа на пристигнатите записи, при што проверува:

1) дали се пополнети задолжителните полиња;
2) дали е применета соодветна категорија и сериозност;
3) дали ознаката за распределба на информации е усогласена со содржината на записот;
4) дали постои поврзаност со друг запис, серија инциденти, кампања, ранливост или закана;
5) дали доставените податоци се доволни за национална евиденција, анализа и известување.

(2) Доколку доставениот запис е непотполн, нејасен или неконзистентен, MKD-CIRT бара дополнување или корекција од изворниот тим, со определување разумен рок кој, по правило, не е подолг од 48 часа.

(3) MKD-CIRT не го менува фактичкиот опис на инцидентот доставен од изворниот тим без консултација со тој тим, освен кога се врши техничка корекција, нормализација на полиња или додавање метаподатоци потребни за Регистарот.

Член 12

(Ажурирање на записите)

(1) Записите во Регистарот се ажурираат при секоја релевантна промена на статусот, сериозноста, опфатот, класификацијата, ознаката за распределба на информации, преземените мерки или исходот на инцидентот.

(2) Ажурирањето го врши изворниот тим, а MKD-CIRT може да изврши ажурирање кога податокот е добиен од надлежен орган, во итна ситуација или кога тоа е неопходно за национална координација.

(3) Секое ажурирање се евидентира со датум и време, идентитет на корисникот, опис на промената и основ за измената.

Член 13

(Корекција и затворање на запис)

(1) Ако се утврди дека записот е дупликат, содржи очигледна грешка или е погрешно класифициран, MKD-CIRT врши корекција или спојување на записите, со зачувување на историјата на измените.

(2) Записот се означува како затворен кога изворниот тим или MKD-CIRT ќе утврди дека постапувањето по инцидентот е завршено и дека се внесени расположливите релевантни податоци.

(3) Затворањето на записот не спречува негово подоцнежно ажурирање ако се појават нови релевантни информации.

IV. ПРИСТАП ДО РЕГИСТАРОТ

Член 14
(Овластени корисници)

(1) Пристап до Регистарот, во обем неопходен за извршување на законските надлежности, може да имаат:

1) MKD-CIRT;
2) Министерството за дигитална трансформација, за потребите на единствената точка за контакт, националното известување, координацијата и подготовката на извештаи согласно Законот;
3) тимовите за одговор на компјутерски инциденти, за записите кои се поврзани со субјектите од нивната надлежност или за анонимизирани и збирни податоци потребни за координација;
4) надлежните органи од член 11 од Законот, за записите кои се однесуваат на субјектите од нивна надлежност;
5) органите од областа на безбедноста, одбраната и спроведувањето на законот, согласно член 16 став (4) од Законот;
6) други органи или субјекти, само доколку пристапот е дозволен со закон, протокол, договор или соодветен правен основ.

(2) Пристапот до Регистарот се заснова на начелата „потреба да се знае" и „најмал неопходен пристап".

(3) Овластувањата за пристап се доделуваат, ревидираат и одземаат согласно интерните процедури на Агенцијата за електронски комуникации и MKD-CIRT.

Член 15
(Нивоа на пристап)

(1) Системот на Регистарот обезбедува нивоа на пристап соодветни на улогата на корисникот и чувствителноста на податоците, и тоа:

1) пристап до анонимизирани и збирни статистички податоци;
2) пристап до ограничени оперативни записи;
3) пристап до целосен запис за конкретен инцидент;
4) административен пристап за управување со системот, без непотребен пристап до содржината на записите;
5) ревизорски пристап за проверка на законитост, безбедност и следливост.

(2) Пристапот до податоци кои содржат лични податоци, деловни тајни, информации за ранливости, безбедносно чувствителни информации или класифицирани информации се ограничува на овластени лица со соодветна законска и оперативна потреба.

Член 16
(Аудиторски траги)

(1) Системот на Регистарот води аудиторски траги за секој внес, преглед, ажурирање, извоз, корекција, бришење на дупликат или административна активност.

(2) Аудиторските траги содржат најмалку: датум и време, идентитет на корисникот, корисничка улога, IP адреса или друг технички идентификатор, тип на активност, идентификатор на засегнатиот запис и резултат на активноста.

(3) Аудиторските траги се заштитуваат од неовластена измена и се прегледуваат периодично за откривање на неовластен, прекумерен или сомнителен пристап.

V. ЗАШТИТА И ЧУВАЊЕ НА ПОДАТОЦИТЕ

Член 17
(Безбедносни мерки)

(1) Агенцијата за електронски комуникации и MKD-CIRT обезбедуваат технички, организациски и оперативни мерки за заштита на Регистарот и податоците во него.

(2) Мерките од ставот 1 на овој член најмалку опфаќаат:

1) силна автентикација и управување со кориснички пристапи;
2) криптографска заштита на податоците при пренос и при чување;
3) сегментација на системот и ограничување на административните привилегии;
4) континуирано следење на безбедносни настани и логови;
5) редовно управување со ранливости, ажурирање и безбедносно зацврстување на системот;
6) периодични безбедносни проверки и тестирања;
7) резервни копии и планови за обновување;
8) процедури за постапување при инцидент кој го засега самиот Регистар.

(3) Безбедносните мерки се утврдуваат согласно ризикот, современите технички достигнувања, Законот, прописите за заштита на личните податоци, прописите за класифицирани информации и применливите европски и меѓународни стандарди.

Член 18
(Континуитет и обновување)

(1) MKD-CIRT обезбедува резервни копии, технички и организациски мерки за континуитет на работењето и план за обновување на Системот на Регистарот во случај на прекин, дефект, сајбер инцидент или катастрофален испад.

(2) Резервните копии се чуваат на безбедна, логички и/или физички одвоена локација и се тестираат периодично.

(3) Планот за континуитет и обновување се тестира најмалку еднаш годишно или по значајна промена на Системот на Регистарот.

Член 19
(Доверливост и класифицирани информации)

(1) Податоците во Регистарот се третираат како податоци со ограничен пристап и се користат само за целите утврдени со Законот и овој правилник.

(2) Доколку податоците во Регистарот содржат класифицирани информации, тие се обработуваат, чуваат, пренесуваат и доставуваат согласно прописите за класифицирани информации.

(3) Доколку податоците содржат деловна тајна, лични податоци, информации за ранливости, индикатори за загрозеност или други безбедносно чувствителни информации, се применуваат соодветни технички и организациски мерки за заштита од неовластено откривање, измена, губење или злоупотреба.

(4) Извештаите, извадоците и аналитичките продукти што произлегуваат од Регистарот се означуваат со соодветна ознака за распределба на информации, вклучително TLP ознака кога е применливо, и со ознака на тајност кога тоа произлегува од закон.

Член 20

(Чување на податоците)

(1) Податоците во Регистарот се чуваат за период потребен за исполнување на целите на Законот, за анализа на трендови, подготовка на извештаи, национална координација, надзор и законски постапки.

(2) Роковите за чување, архивирање, ограничување на пристап и бришење на податоците се уредуваат со внатрешен акт на Агенцијата за електронски комуникации, во согласност со прописите за архивско работење, заштита на лични податоци, класифицирани информации и други применливи прописи.

(3) Податоците кои повеќе не се неопходни во идентификувачка форма се анонимизираат или се обработуваат како збирни статистички податоци, кога тоа е можно и соодветно.

VI. ИЗВЕШТАИ, АНАЛИТИКА И РАЗМЕНА НА ПОДАТОЦИ

Член 21

(Извештаи)

(1) Врз основа на податоците од Регистарот, MKD-CIRT изготвува редовни, периодични и вонредни извештаи.

(2) Извештаите од ставот 1 на овој член може да опфаќаат:

1) оперативни извештаи за потребите на MKD-CIRT;
2) извештаи за потребите на Мрежата на тимови за одговор на компјутерски инциденти;
3) секторски извештаи за надлежните органи;
4) полугодишни и годишни извештаи до Министерството за дигитална трансформација согласно член 16 став (3) од Законот;
5) збирни и анонимизирани податоци за Годишниот извештај за состојбите во сајбер безбедноста;
6) вонредни извештаи на барање на Министерството, надлежен орган, Тимот за координација или друг овластен орган согласно закон.

(3) Извештаите не содржат лични податоци, деловни тајни, класифицирани информации или безбедносно чувствителни информации, освен кога тоа е неопходно, законски дозволено и соодветно заштитено.

Член 22

(Аналитички продукти)

(1) MKD-CIRT може да изготвува аналитички продукти врз основа на податоците од Регистарот, вклучувајќи анализи на трендови, типови инциденти, засегнати области, закани, ранливости, индикатори, тактики, техники, процедури и препорачани мерки.

(2) Аналитичките продукти се распределуваат селективно, согласно потребата да се знае, применливата TLP ознака и правилата за доверливост, до релевантни субјекти, надлежни органи, тимови за одговор на компјутерски инциденти и други засегнати страни.

Член 27
(Влегување во сила)

Овој правилник влегува во сила од денот на неговото објавување на огласната табла/веб-страницата на Агенцијата а електронски комуникации и MKD-CIRT.

Изработил,
Sevdali Selmani
Проверил,
Бојана Стефановска

ДИРЕКТОР
на Агенцијата за електронски комуникации
Nusret Haliti

Бр. 0101-1717/2
Скопје, 25.06.2026 година