Врз основа на член 22 став (3) од Законот за безбедност на мрежни и информациски системи („Службен весник на Република Северна Македонија" бр. 135/2025), а во врска со член 11 став (1) точка 2), член 15 став (3), член 16 став (1), член 20 став (1), член 21, член 23 ставови (1), (2), (3), (4) и (5), член 24, член 33 и член 38 од истиот закон, директорот на Агенцијата за електронски комуникации донесе

ПРАВИЛНИК

ЗА НАЧИНОТ НА ПРИЈАВА И ПОСТАПУВАЊЕ ПО ПРИЈАВЕНИ ИЛИ ИДЕНТИФИКУВАНИ ИНЦИДЕНТИ НА МРЕЖНИТЕ И ИНФОРМАЦИСКИТЕ СИСТЕМИ ВО НАЦИОНАЛНИОТ ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ (MKD-CIRT)

I. ОПШТИ ОДРЕДБИ

Член 1

(Предмет)

(1) Со овој правилник се уредуваат начинот на пријава, прием, потврдување, тријажа, иницијална и оперативна класификација, ескалација, постапување, координација, известување, затворање и по-инцидентна анализа на пријавени или идентификувани инциденти на мрежните и информациските системи во Националниот центар за одговор на компјутерски инциденти (во натамошниот текст: MKD-CIRT).

(2) Овој правилник се применува и на постапувањето со значајни сајбер закани, избегнати инциденти и пријави за ранливости, кога нивната обработка е поврзана со спречување, откривање, анализа, ублажување или справување со инцидент, како и со обврските на MKD-CIRT согласно Законот за безбедност на мрежни и информациски системи (во натамошниот текст: Законот).

(3) Овој правилник не ја уредува формата, содржината и начинот на водење на евиденцијата на пријавени инциденти, ниту формата, содржината и начинот на водење на Националниот регистар на сајбер инциденти, кои се уредуваат со посебни акти донесени врз основа на член 16 ставови (5) и (6) од Законот.

Член 2

(Опфат и применливост)

(1) Овој правилник се применува на постапувањето на MKD-CIRT по инциденти кои се однесуваат на субјектите од надлежност на Агенцијата за електронски комуникации, преку MKD-CIRT, согласно член 11 став (1) точка 2) и член 20 став (1) од Законот.

(2) Овој правилник се применува и кога MKD-CIRT постапува во координација со Министерството за дигитална трансформација, MKD-GOV-CSIRT, секторски CSIRT, други надлежни органи, органи од областа на безбедноста, одбраната и спроведувањето на законот, Народната банка, партнерски CSIRT и меѓународни организации, во рамките на законските надлежности.

(3) При примената на овој правилник се земаат предвид релевантните европски и меѓународни стандарди и добри практики за управување со инциденти, вклучително ISO/IEC 27035, NIST SP 800-61, референтните таксономии на ENISA, FIRST TLP 2.0, MITRE ATT&CK и други применливи технички спецификации, доколку не се спротивни на Законот и на националните стандарди утврдени согласно член 23 став (5) од Законот.

Член 3

(Усогласување со стандардизираните практики од член 23 став (5) од Законот)

(1) Постапувањето по овој правилник задолжително се усогласува со заедничките или стандардизираните практики, шемите за класификација и класификациите што ги утврдува MKD-CIRT согласно член 23 став (5) од Законот, особено во однос на:

1. процедурите за справување со инциденти;
2. управувањето со кризи; и
3. координираното откривање на ранливости.

(2) Класификациската матрица, фазите на справување, ескалациските правила, TLP-ознаките, процедурите за кризно управување и постапката за координирано откривање на ранливости од овој правилник се применуваат како оперативна рамка на MKD-CIRT и се усогласуваат со стандардите од ставот (1) на овој член.

(3) Доколку по донесувањето на овој правилник MKD-CIRT утврди или измени стандардизирани практики, шеми за класификација или класификации согласно член 23 став (5) од Законот, оперативните прилози, внатрешните процедури и техничките упатства што произлегуваат од овој правилник се усогласуваат со тие стандарди во рок од 60 дена од нивното донесување, освен ако со самиот стандард не е утврден друг рок.

(4) До донесување на целосните стандарди од член 23 став (5) од Законот, MKD-CIRT ги применува класификациите и процедурите од овој правилник како преодна оперативна рамка, без да се ограничува законската можност за нивно дополнително стандардизирање на национално ниво.

Член 4

(Начела на постапување)

MKD-CIRT постапува согласно следните начела:

1) законитост — секое постапување се врши во рамките на надлежностите утврдени со Законот;

2) навременост — пријавите се примаат, тријажираат и обработуваат без непотребно одлагање;

3) пропорционалност — интензитетот на постапувањето се определува според сериозноста, влијанието и ризикот од инцидентот;

4) доверливост — добиените информации се користат само за законски утврдени цели и се споделуваат според TLP-ознаката, степенот на тајност и принципот „потреба да се знае";

5) минимизација на податоци — се обработуваат само податоците неопходни за прием, анализа, справување, известување и документирање;

6) интегритет на доказите — техничките артефакти и доказите се прибираат, чуваат и обработуваат на начин што овозможува проверливост и зачувување на нивниот интегритет;

7) координација — постапувањето се врши во соработка со засегнатиот субјект, надлежните органи и другите тимови за одговор на компјутерски инциденти, кога тоа е потребно;

8) непреземање истражни овластувања — MKD-CIRT не врши кривична истрага и не презема дејствија кои се во надлежност на органите за гонење, туку дава насоки и техничка поддршка во рамките на Законот;

9) континуитет на услугата — постапувањето треба да придонесе кон спречување, ублажување и ограничување на влијанието врз услугите на засегнатиот субјект;

10) усогласеност со член 23 став (5) од Законот — сите оперативни класификации и процедури се усогласуваат со стандардизираните практики и шеми утврдени од MKD-CIRT.

II. КАНАЛИ И НАЧИН НА ПРИЈАВУВАЊЕ

Член 5

(Канали за пријавување)

(1) MKD-CIRT обезбедува повеќе канали за прием на пријави, достапни на начин кој обезбедува континуитет на комуникацијата и отпорност на прекин на поединечен канал.

(2) Пријавите може да се доставуваат преку:

1) единствениот портал за сајбер безбедност, кога е воспоставен и функционален за оваа намена;

2) наменска електронска адреса за пријавување инциденти, со можност за криптографска заштита на содржината;

3) телефонски канал за итни инциденти;

4) писмено известување, вклучително и преку архивата на Агенцијата, кога тоа е соодветно според природата на пријавата;

5) технички интерфејс или платформа за машински читлива размена на податоци, кога е воспоставена;

6) проследување од друг надлежен орган, тим за одговор на компјутерски инциденти или партнерска институција; и

7) доброволно известување од субјект, физичко лице, правно лице, истражувач или трета страна.

(3) Каналите за комуникација се објавуваат на интернет-страницата на MKD-CIRT и на Агенцијата и се ажурираат без одлагање при секоја промена.

(4) Кога пријавата содржи класифицирани информации, се користат канали и системи што ги исполнуваат условите согласно прописите за класифицирани информации.

Член 6

(Минимална содржина на пријавата)

(1) Пријавата за инцидент, доколку податоците се познати во моментот на пријавување, содржи:

1) назив, седиште, електронска адреса и контакт-телефон на засегнатиот субјект;

2) име, презиме, функција и контакт на лицето кое ја доставува пријавата, освен кај анонимни пријави;

3) датум и време на откривање, настанување или првично забележување на инцидентот;

4) краток опис на инцидентот, засегнатата услуга, систем, мрежа, апликација или податок;

5) почетна проценка на влијанието врз доверливоста, интегритетот, достапноста, корисниците и услугите;

6) информација дали постои сомневање за незаконско или злонамерно дејствување;

7) информација дали постои можност за прекугранично влијание;

8) познати индикатори за загрозеност, артефакти, логови, пораки, датотеки, IP-адреси, домени, URL-адреси или хеш-вредности;

9) мерки што веќе се преземени од засегнатиот субјект;

10) барање за техничка или координативна поддршка, доколку таква поддршка се бара;

11) TLP-ознака или друга ознака за ограничување на споделувањето, доколку е применливо.

(2) Недоставувањето на сите податоци од ставот (1) на овој член не е причина за неприемање на пријавата. MKD-CIRT може дополнително да побара појаснување или дополнување на податоците.

(3) За значајни сајбер безбедносни инциденти се применуваат роковите и содржината на известувањата утврдени со член 33 од Законот и со методологиите донесени согласно член 33 став (12) од Законот.

Член 7

(Анонимни и доверливи пријави)

(1) MKD-CIRT може да прима анонимни и доверливи пријави, особено кога се однесуваат на ранливости, сајбер закани, избегнати инциденти или информации што може да придонесат кон спречување или ублажување на инцидент.

(2) Кога идентитетот на пријавителот е познат, MKD-CIRT го штити неговиот идентитет и не го открива без согласност на пријавителот, освен кога откривањето е потребно врз основа на закон.

(3) Анонимните пријави за ранливости се обработуваат согласно член 24 од Законот и стандардизираните практики за координирано откривање на ранливости утврдени согласно член 23 став (5) од Законот.

III. ПРИЕМ, ПОТВРДУВАЊЕ И ТРИЈАЖА

Член 8

(Прием и потврдување на пријавата)

(1) По приемот на пријава, MKD-CIRT врши иницијална проверка на каналот, изворот, содржината, TLP-ознаката и евентуалната итност на пријавата.

(2) Кога е возможно, MKD-CIRT го потврдува приемот на пријавата до пријавителот без непотребно одлагање. За пријави кои очигледно укажуваат на значаен инцидент, потврдувањето се врши приоритетно.

(3) Приемот на пријавата се документира во оперативната евиденција на MKD-CIRT со датум, време, канал, извор и почетна TLP-ознака, согласно правилникот донесен врз основа на член 16 став (5) од Законот.

(4) Автоматска потврда преку портал или технички интерфејс не претставува конечна оценка за веродостојност, значајност или класификација на пријавениот настан.

Член 9

(Тријажа)

(1) Тријажата е иницијална стручна проценка со која MKD-CIRT утврдува дали пријавениот или идентификуваниот настан претставува инцидент, значајна сајбер закана, избегнат инцидент, ранливост, лажна пријава, дупликат или информација од оперативно значење.

(2) Тријажата опфаќа:

1) проверка на комплетноста и веродостојноста на достапните податоци;

2) проверка дали настанот спаѓа во надлежност на MKD-CIRT;

3) проверка на можни поврзани записи, кампањи или повторени пријави;

4) иницијална класификација според тип на настан и сериозност;

5) иницијална проценка дали настанот може да претставува значаен сајбер безбедносен инцидент;

6) иницијална проценка на можност за прекугранично влијание;

7) одредување на потреба од ескалација, известување или техничка поддршка;

8) одредување на одговорно лице или тим за понатамошно постапување.

(3) Тријажата се врши според стандардизирана шема за класификација утврдена согласно член 23 став (5) од Законот. До нејзиното целосно утврдување, се применува матрицата од Прилог 1 на овој правилник.

Член 10

(Класификација на настанот)

(1) Пријавениот или идентификуваниот настан се класифицира според две основни димензии:

1) тип на настан: инцидент, значајна сајбер закана, избегнат инцидент, ранливост, информација за индикатори, лажна пријава или дупликат;

2) ниво на сериозност: критично, високо, средно, ниско или информативно.

(2) Класификацијата се усогласува со националните стандардизирани практики и шеми за класификација од член 23 став (5) од Законот, со методологиите за определување на обични и значајни инциденти од член 33 став (12) од Законот и со релевантните таксономии на ENISA и FIRST, доколку се применливи.

(3) Промената на класификацијата во текот на постапувањето се документира со образложение, датум, време и лице кое ја извршило промената.

Член 11

(Приоритет и ескалација)

(1) Приоритетот на постапување се определува врз основа на сериозноста, видот на засегнатиот субјект, влијанието врз услугите, постоењето на прекугранично влијание, можноста за ширење, степенот на доверба во податоците и можноста за настанување на инцидент со голем опфат или сајбер криза.

(2) Инцидентите со критично или високо ниво на сериозност се ескалираат до раководителот на MKD-CIRT или до друго овластено лице, согласно внатрешните процедури.

(3) Инцидентите со можен голем опфат, со прекугранично влијание, со влијание врз повеќе сектори или со можни последици по јавната безбедност, јавната заштита, јавното здравје, националната безбедност или функционирањето на критични услуги се ескалираат и координираат согласно стандардите за управување со кризи од член 23 став (5) од Законот и Планот од член 30 од Законот, кога е применливо.

IV. ПОСТАПУВАЊЕ И СПРАВУВАЊЕ СО ИНЦИДЕНТИ

Член 12

(Фази на постапување)

(1) Постапувањето на MKD-CIRT се организира во следните фази:

1) прием и евидентирање на пријавата;

2) тријажа, иницијална класификација и приоритизација;

3) техничка анализа, корелација и проценка на влијанието;

4) спречување, ограничување или ублажување на инцидентот, во соработка со засегнатиот субјект;

5) поддршка при отстранување на причините и закрепнување;

6) известување, координација и размена на информации;

7) затворање и по-инцидентна анализа.

(2) Фазите од ставот (1) на овој член се применуваат пропорционално, зависно од природата и сериозноста на инцидентот.

(3) Деталните оперативни чекори за секоја фаза се уредуваат со стандардизирани практики и интерни процедури усогласени со член 23 став (5) од Законот.

Член 13

(Распределба на предметот)

(1) По тријажата, предметот се распределува на одговорен аналитичар или тим за постапување, зависно од сериозноста и потребната експертиза.

(2) За значајни инциденти, инциденти со висок ризик или инциденти кои бараат повеќе дисциплини, раководителот на MKD-CIRT може да определи тим за постапување составен од лица со соодветни технички, правни, комуникациски или координативни компетенции.

(3) Кога е потребна експертиза која не е достапна во MKD-CIRT, може да се побара поддршка од други надлежни органи, партнерски CSIRT, надворешни експерти или меѓународни партнери, согласно закон, TLP-ознаката, правилата за доверливост и заштита на податоци.

Член 14

(Поддршка на засегнатиот субјект)

(1) MKD-CIRT, во рамките на своите капацитети и надлежности, обезбедува насоки, оперативни совети и техничка поддршка на засегнатиот субјект.

(2) Поддршката може да опфати:

1) иницијални насоки за спречување, ограничување или ублажување;

2) анализа на доставени индикатори, логови, артефакти, пораки или злонамерни датотеки;

3) споделување индикатори за загрозеност, тактики, техники и процедури;

4) координација со други тимови за одговор на компјутерски инциденти;

5) насоки за известување на корисници, добавувачи или надлежни органи;

6) препораки за обновување, континуитет на работењето и спречување на повторување;

7) проактивно ненаметливо скенирање на јавно достапни мрежни и информациски системи, кога се исполнети условите од член 23 став (2) од Законот.

(3) Поддршката од MKD-CIRT не ја заменува одговорноста на засегнатиот субјект за управување со сопствените мрежни и информациски системи, спроведување мерки за сајбер безбедност и исполнување на законските обврски за известување.

Член 15

(Постапување со технички артефакти и докази)

(1) Техничките артефакти и доказите доставени до MKD-CIRT се обработуваат на начин кој го зачувува нивниот интегритет, автентичност и употребливост за анализа.

(2) За доставени артефакти, кога е применливо, се бележат извор, датум и време на прием, опис, хеш-вредност, лице кое го примило артефактот, TLP-ознака и ограничувања за користење.

(3) Ако артефактите содржат лични податоци, деловна тајна или класифицирани информации, MKD-CIRT применува соодветни мерки за заштита согласно релевантните прописи.

(4) MKD-CIRT не презема процесни дејствија што се во надлежност на органите за гонење. Доколку постои сомневање за кривично дело, се постапува согласно член 20 од овој правилник.

V. ИЗВЕСТУВАЊА, КООРДИНАЦИЈА И КОМУНИКАЦИЈА

Член 16

(Известувања од суштински и важни субјекти)

(1) MKD-CIRT прима известувања од суштинските и важните субјекти согласно член 33 од Законот, вклучително иницијално известување, рано предупредување, известување за инцидентот, привремено известување, завршно известување, извештај за напредок и завршен извештај.

(2) При прием на известување од ставот (1) на овој член, MKD-CIRT проверува дали известувањето содржи доволно информации за утврдување на сериозноста, влијанието, прекуграничното влијание и потребата од координација со други органи.

(3) Кога известувањето е непотполно, MKD-CIRT може да побара дополнителни информации, без тоа да влијае врз веќе започнатото постапување.

Член 17

(Одговор на MKD-CIRT)

(1) MKD-CIRT доставува повратни информации, насоки или оперативни совети до засегнатиот субјект согласно член 33 ставови (5), (6) и (7) од Законот.

(2) Одговорот на MKD-CIRT може да содржи:

1) потврда на прием;

2) иницијална проценка и препорачани итни мерки;

3) барање за дополнителни информации;

4) насоки за зачувување докази и технички артефакти;

5) препораки за спречување, отстранување, закрепнување и известување;

6) предлог за координација со други субјекти или органи.

(3) Одговорот се документира во оперативната евиденција на MKD-CIRT.

Член 18

(Известување на Министерството како единствена точка за контакт)

(1) MKD-CIRT го информира Министерството за дигитална трансформација, како единствена точка за контакт, за инциденти, сајбер закани и избегнати инциденти поднесени согласно Законот.

(2) За значајни инциденти со прекугранично влијание, MKD-CIRT го известува Министерството без непотребно одлагање, со податоците неопходни за натамошно известување на засегнатите држави согласно Законот.

(3) Во роковите утврдени со Законот, MKD-CIRT доставува детални извештаи до Министерството за инциденти со прекугранично влијание и за други инциденти кога тоа е потребно за извршување на функцијата на единствена точка за контакт.

Член 19

(Координација со други тимови и надлежни органи)

(1) Кога инцидентот се однесува на субјекти од различна надлежност, MKD-CIRT координира со MKD-GOV-CSIRT, секторски CSIRT, надлежни органи и други релевантни тела, согласно Законот и стандардизираните практики од член 23 став (5) од Законот.

(2) Координацијата може да опфати размена на технички информации, индикатори, предупредувања, заедничка анализа, усогласени препораки, оперативни состаноци и заедничко постапување во рамките на Мрежата на тимови за одговор на компјутерски инциденти.

(3) Размената на информации се врши со почитување на TLP-ознаките, класифицираните информации, деловната тајна, личните податоци и ограничувањата поврзани со националната безбедност, јавната безбедност и одбраната.

Член 20

(Сомневање за кривично дело)

(1) Кога постои сомневање дека со значаен сајбер безбедносен инцидент е сторено кривично дело, MKD-CIRT му дава насока на засегнатиот субјект инцидентот да го пријави кај надлежните органи, согласно член 33 став (8) од Законот.

(2) MKD-CIRT може, на барање на надлежните органи, да обезбеди техничка поддршка, информации или експертско појаснување во рамките на своите надлежности и согласно прописите за заштита на податоци, класифицирани информации и деловна тајна.

(3) Постапувањето по ставот (2) на овој член не претставува преземање на истражни дејствија од страна на MKD-CIRT.

Член 21

(Комуникација со јавноста)

(1) Кога за спречување или решавање на значаен сајбер безбедносен инцидент е потребно известување на јавноста, MKD-CIRT постапува во координација со Министерството и по консултација со засегнатиот субјект, согласно член 33 став (10) од Законот.

(2) MKD-CIRT не објавува идентификабилни информации за засегнати субјекти, технички ранливости, индикатори или податоци што може да го зголемат ризикот, освен кога тоа е неопходно и дозволено согласно закон.

(3) Јавните информации се подготвуваат на разбирлив јазик, со точни и проверени податоци, и се означуваат како TLP:CLEAR кога се наменети за јавна објава.

VI. УПРАВУВАЊЕ СО ИНЦИДЕНТИ СО ГОЛЕМ ОПФАТ И САЈБЕР КРИЗИ

Член 22

(Инциденти со голем опфат и сајбер кризи)

(1) Доколку инцидентот има или може да има голем опфат, системско влијание, прекугранично влијание или карактеристики на сајбер криза, MKD-CIRT веднаш го ескалира случајот до раководителот на MKD-CIRT и го известува Министерството за дигитална трансформација.

(2) Во случаите од ставот (1) на овој член, MKD-CIRT постапува согласно Законот, Планот за одговор на сајбер безбедносни закани, значајни сајбер безбедносни закани, значајни сајбер безбедносни инциденти, сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи, како и стандардизираните практики за управување со кризи утврдени согласно член 23 став (5) од Законот.

(3) Кога е воспоставен Тим за координација на одговор по инциденти со голем опфат и кризни состојби, MKD-CIRT обезбедува поддршка и информации во рамките на своите надлежности.

Член 23

(Кризна координација и стандардизирани практики)

(1) За потребите на кризна координација, MKD-CIRT применува заеднички класификации, стандардизирани статуси на инцидент, ескалациски нивоа, комуникациски протоколи и TLP-правила утврдени согласно член 23 став (5) од Законот.

(2) Стандардизираните практики за управување со кризи најмалку треба да опфатат:

1) критериуми за ескалација од оперативен инцидент во инцидент со голем опфат или сајбер криза;

2) улоги и одговорности на MKD-CIRT, MKD-GOV-CSIRT, надлежните органи и други тимови;

3) начин на изготвување и размена на ситуациски извештаи;

4) комуникациски канали и резервни канали;

5) правила за заедничка анализа, јавна комуникација и меѓународна координација;

6) постапка за по-кризна анализа и научени поуки.

VII. КООРДИНИРАНО ОТКРИВАЊЕ НА РАНЛИВОСТИ

Член 24

(Улога на MKD-CIRT)

(1) MKD-CIRT е координатор во процесот на координирано откривање на ранливости кај ИКТ-производи или ИКТ-услуги, доколку откривањето на ранливости со друг закон не е поинаку уредено.

(2) При постапување со пријави за ранливости, MKD-CIRT ги применува стандардизираните практики за координирано откривање на ранливости утврдени согласно член 23 став (5) од Законот и задачите од член 24 од Законот.

(3) MKD-CIRT може да постапува како посредник помеѓу лицето кое ја пријавува ранливоста и производителот, давателот на услуга или друг засегнат субјект, кога тоа е потребно за координирано управување со ранливоста.

Член 25

(Постапка за координирано откривање на ранливости)

(1) Постапката за координирано откривање на ранливости опфаќа:

1) прием и иницијална проверка на пријавата;

2) утврдување на засегнати производи, услуги, системи или субјекти;

3) контактирање со засегнатите субјекти;

4) координација на временските рокови за проверка, корекција и евентуално обелоденување;

5) заштита на анонимноста на пријавителот, кога пријавата е анонимна или доверлива;

6) координација со други национални или странски CSIRT кога ранливоста има влијание во повеќе држави;

7) документирање на исходот, научените поуки и препорачаните мерки.

(2) Јавно обелоденување на ранливост се врши само кога тоа е усогласено со засегнатите страни или кога постои оправдан јавен интерес, при што се води сметка да не се зголеми ризикот за корисниците и системите.

VIII. ЗАТВОРАЊЕ, ПО-ИНЦИДЕНТНА АНАЛИЗА И ПОКАЗАТЕЛИ

Член 26

(Затворање на инцидентот)

(1) Инцидентот се затвора кога MKD-CIRT, врз основа на достапните информации, ќе утврди дека се завршени релевантните активности за постапување, координација и известување.

(2) За затворање на инцидентот, кога е применливо, се проверува дали:

1) заканата е ограничена или отстранета;

2) засегнатиот субјект презел или планира соодветни мерки за ублажување;

3) потребните известувања се доставени;

4) доставените артефакти и податоци се обработени или архивирани;

5) потребните препораки се дадени;

6) предметот е документиран во оперативната евиденција.

(3) Затворен предмет може повторно да се отвори ако се појават нови релевантни податоци, поврзан инцидент, нова ранливост, барање од надлежен орган или потреба од дополнителна анализа.

Член 27

(Пост-инцидентна анализа)

(1) За значајни инциденти, инциденти со голем опфат, инциденти со прекугранично влијание или инциденти од кои произлегуваат важни системски поуки, MKD-CIRT изготвува пост-инцидентна анализа;

(2) Пост-инцидентна анализа може да содржи:

1) краток опис на инцидентот и временска линија;

2) причини и придонесувачки фактори;

3) оценка на влијанието;

4) оценка на постапувањето и координацијата;

5) технички и организациски пропусти;

6) научени поуки;

7) препораки за засегнатиот субјект, секторот или националната рамка.

(3) Наодите од пост-инцидентната анализа кои имаат пошироко значење може да се користат во збирна или анонимизирана форма за извештаи, предупредувања, упатства, обуки и подобрување на стандардизираните практики од член 23 став (5) од Законот.

Член 28

(Показатели за изведба)

(1) MKD-CIRT може да следи показатели за изведба со цел подобрување на сопственото постапување, вклучително:

1) просечно време до потврдување на прием;

2) просечно време до завршување на тријажа;

3) просечно време до прва оперативна препорака;

4) просечно време до ограничување или ублажување, кога MKD-CIRT има релевантни податоци;

5) просечно време до затворање на предмет;

6) број и процент на значајни инциденти, избегнати инциденти, прекугранични инциденти и CVD-предмети;

7) степен на усогласеност со роковите и обврските од Законот.

(2) Показателите од ставот (1) на овој член се користат за внатрешно подобрување, извештаи и планирање, без да создаваат дополнителни обврски за засегнатите субјекти надвор од Законот.

IX. ДОВЕРЛИВОСТ, ЗАШТИТА НА ПОДАТОЦИ И ДОКУМЕНТИРАЊЕ

Член 29

(Доверливост и TLP)

(1) Сите информации добиени или создадени во постапувањето по инциденти се третираат согласно нивната чувствителност, TLP-ознака, степен на тајност, деловна тајна и законските ограничувања за пристап и споделување.

(2) Информации означени како TLP:RED или со еквивалентно ограничување не се споделуваат надвор од кругот на лицата кои се изречно овластени и имаат оперативна потреба да ги знаат.

(3) Информациите за ранливости, индикатори, техники на напад или неотстранети слабости се споделуваат само во обем што е неопходен за превенција, откривање, справување или ублажување на ризик.

Член 30

(Заштита на лични податоци и класифицирани информации)

(1) Личните податоци што се обработуваат при постапувањето се ограничуваат на она што е неопходно за целите на Законот и овој правилник.

(2) Кога инцидентот вклучува или може да вклучува повреда на безбедноста на личните податоци, MKD-CIRT постапува во согласност со Законот, прописите за заштита на лични податоци и надлежностите на Агенцијата за заштита на личните податоци.

(3) Кога информациите се класифицирани или може да бидат класифицирани, се применуваат прописите за класифицирани информации и се користат соодветни безбедносни канали и системи.

Член 31

(Документирање)

(1) Секој предмет се документира во оперативната евиденција на MKD-CIRT, со сите релевантни податоци за прием, тријажа, класификација, преземени активности, известувања, комуникација, технички артефакти, препораки, затворање и поуки.

(2) Податоците потребни за Националниот регистар на сајбер инциденти се доставуваат или генерираат согласно правилникот донесен врз основа на член 16 став (6) од Законот и техничките правила за поврзување со единствениот портал за сајбер безбедност.

(3) Документирањето се врши на начин кој овозможува проверливост, континуитет, ревизиска трага и подготовка на полугодишни, годишни, вонредни или други извештаи согласно Законот.

X. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 32

(Усогласување со постојни процедури)

(1) Постојните оперативни процедури, обрасци, класификациски шеми, ескалациски матрици и комуникациски протоколи на MKD-CIRT се усогласуваат со овој правилник во рок од три месеци од денот на неговото влегување во сила.

(2) До завршување на усогласувањето, постојните процедури се применуваат во делот во кој не се во спротивност со Законот и со овој правилник.

Член 33

(Усогласување со стандардите од член 23 став (5))

(1) По донесување или измена на стандардизираните практики, шеми за класификација и класификации од член 23 став (5) од Законот, MKD-CIRT ги усогласува прилозите, интерните процедури и техничките упатства што произлегуваат од овој правилник.

(2) Усогласувањето од ставот (1) на овој член особено се однесува на:

1) класификацијата на инциденти и сајбер закани;

2) стандардните фази и активности за справување со инциденти;

3) ескалацијата и управувањето со инциденти со голем опфат и сајбер кризи;

4) координираното откривање на ранливости;

5) TLP и правилата за споделување информации;

6) извештаите, обрасците и техничките формати за размена.

Член 34

(Влегување во сила)

Овој правилник влегува во сила со денот на неговото објавување на веб страната на Агенцијата а електронски комуникации и MKD-CIRT.

Бр. 0101-1513/17

14.07. 2026 година

Скопје

Директор

на Агенцијата за електронски комуникации

Nusret Haliti

Изготвил:

Раководител на MKD-CIRT
Sevdali Selmani

ПРИЛОГ 1 — ПРЕОДНА КЛАСИФИКАЦИСКА МАТРИЦА

Оваа матрица се применува до целосно утврдување или ажурирање на стандардизираните практики, шеми за класификација и класификации од член 23 став (5) од Законот.

Ниво	Ознака	Опис	Типични активности
Критично	C	Значајно нарушување на критична или суштинска услуга со национално, системско или прекугранично влијание, или можност за инцидент со голем опфат/сајбер криза.	Итна ескалација, известување на Министерството, координација со засегнати тимови и органи, ситуациски извештаи.
Високо	H	Значаен инцидент кај суштински субјект, оператор на критична инфраструктура или субјект со потенцијал за прекугранично или секторско влијание.	Приоритетна тријажа, оперативна поддршка, следење на рокови од член 33, координација со надлежни органи.
Средно	M	Инцидент кај важен или друг релевантен субјект со ограничено влијание, но со потенцијал за ескалација ако не се преземат мерки.	Редовна обработка, препораки, мониторинг, ажурирање на евиденција.
Ниско	L	Локален или ограничен инцидент без значајно влијание и без јасен потенцијал за ескалација.	Основна обработка, препораки, затворање по потврда.
Информативно	I	Информација, индикатор, избегнат инцидент, ранливост или настан без непосредно нарушување, но со превентивно или аналитичко значење.	Документирање, корелација, евентуално предупредување или CVD-постапување.

ПРИЛОГ 2 — МИНИМАЛНА ЛИСТА НА СТАТУСИ НА ПРЕДМЕТ

Статус	Значење
Примено	Пријавата е примена, но не е завршена иницијалната проверка.
Во тријажа	Се врши иницијална проценка и класификација.
Во постапување	Се врши техничка анализа, координација или поддршка.
Ескалирано	Предметот е ескалиран поради значајност, прекугранично влијание, кризен потенцијал или потреба од координација.
Ограничено/ублажено	Достапните податоци укажуваат дека влијанието е ограничено или ублажено.
Затворено	Постапувањето е завршено и предметот е документиран.
Повторно отворено	Предметот е повторно отворен поради нови факти или поврзан настан.

ПРИЛОГ 3 — ОБЛАСТИ ЗА УСОГЛАСУВАЊЕ СО ЧЛЕН 23 СТАВ (5) ОД ЗАКОНОТ

При утврдување на стандардизираните практики, шеми за класификација и класификации од член 23 став (5) од Законот, овој правилник треба оперативно да се усогласи најмалку во следните области:

1) единствена национална таксономија на инциденти, сајбер закани, избегнати инциденти и ранливости;

2) единствена матрица за сериозност и влијание;

3) заеднички статуси на предмети и ескалациски нивоа;

4) заеднички правила за TLP и споделување информации;

5) минимални податоци за известувања и оперативни извештаи;

6) стандардни процедури за справување со инциденти;

7) стандардни процедури за управување со сајбер кризи и инциденти со голем опфат;

8) стандардна CVD-постапка, вклучително рокови, комуникација, анонимност и координирано обелоденување;

9) машински читливи формати и канали за размена, кога се користат технички платформи;

10) постапки за по-инцидентна анализа и научени поуки.