Врз основа на член 23 став (5) 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 утврдување на стандардизирани практики, шеми за класификација и класификации на национално ниво за тимовите за одговор на компјутерски инциденти

I. ОПШТИ ОДРЕДБИ

Член 1
(Предмет)

(1) Со овој правилник се утврдуваат стандардизираните практики, шемите за класификација и класификациите на национално ниво кои ги применуваат тимовите за одговор на компјутерски инциденти во Република Северна Македонија, заради олеснување на нивната меѓусебна соработка, размена на информации, координирано справување со инциденти, управување со сајбер безбедносни кризи и координирано откривање на ранливости.

(2) Правилникот ги уредува најмалку: националната таксономија на инциденти, скалата на сериозност, минималните содржински елементи на записите, примената на TLP ознаки, стандардизираните фази за справување со инциденти, стандардите за кризно справување, стандардите за координирано откривање на ранливости и форматите за техничка размена на информации.

(3) Овој правилник не ги заменува посебните оперативни процедури на одделните тимови, туку утврдува заедничка национална рамка која тие процедури мора да ја почитуваат.

Член 2
(Цел)

Целта на овој правилник е да обезбеди единствена национална, терминолошка и процедурална рамка како и споредливи процедури за постапување на сите тимови за одговор на компјутерски инциденти, со што се овозможува:

1) меѓуоперабилност на евиденциите, регистрите и техничките системи;
2) еднообразна класификација на инциденти, ранливости и закани;
3) споредливи статистики и аналитички продукти на национално ниво;
4) побрзо меѓутимско ескалирање и координирано делување;
5) усогласување со релевантните европски и меѓународни практики, особено ENISA, FIRST.Org, ISO/IEC, NIST, MITRE и OASIS стандардите; и
6) подготовка на националните тимови за соработка со европските и меѓународните CSIRT мрежи.

Член 3
(Применливост)

(1) Овој правилник го применуваат MKD-CIRT, MKD-GOV-CSIRT, секторските тимови за одговор на компјутерски инциденти, како и другите тимови за одговор на компјутерски инциденти воспоставени согласно Законот или посебни прописи.

(2) За тимовите во рамките на органите од областа на безбедноста, одбраната, органот кој ги гони сторителите на кривични дела и Народната банка, овој правилник се применува во делот во кој не е во спротивност со посебните закони, прописите за класифицирани информации и правилата за заштита на оперативно чувствителни податоци.

(3) Кога одделен тим применува секторски или внатрешни класификациски шеми, тие мора да бидат мапирани со националните шеми утврдени со овој правилник.

Член 4
(Дефиниции)

Изразите употребени во овој правилник го имаат значењето утврдено во Законот. За целите на овој правилник, дополнително се применуваат следните поими:

Поим	**Значење**
стандардизирана практика	усогласен начин на постапување што го применуваат сите тимови при прием, класификација, ескалација, размена и затворање на инциденти;
шема за класификација	структуриран систем на категории, подкатегории, ознаки и критериуми со кој инцидентите, ранливостите, заканите или информациите се класифицираат на споредлив начин;
таксономија	хиерархиски уредена класификација на типови инциденти, заснована на ENISA Reference Security Incident Taxonomy (RSIT), приспособена за национална примена;
сериозност	ниво на влијание и итност на инцидентот, определено според заедничката петстепена скала од овој правилник;
TLP	Traffic Light Protocol, верзија 2.0 на FIRST.Org, кој го определува дозволениот опсег на дистрибуција на споделените информации;
CVD	координирано откривање на ранливости (Coordinated Vulnerability Disclosure), односно постапка за прием, валидација, координација и обелоденување на ранливости;
IOC	индикатор за загрозеност (Indicator of Compromise), технички податок кој укажува на можна компромитација, напад или злонамерна активност;
TTP	тактики, техники и процедури на заканувар, најчесто мапирани со MITRE ATT&CK рамката;

Член 5
(Принципи)

Принцип	**Содржина**

законитост	стандардизацијата се врши во рамки на надлежностите утврдени со Законот;
меѓуоперабилност	категориите, полињата и форматите мора да овозможуваат техничка и семантичка размена меѓу тимовите;
пропорционалност	степенот на класификација, ескалација и размена мора да биде сразмерен на ризикот и влијанието;
навременост	класификацијата и размената се вршат без непотребно одложување;
доверливост и потреба да се знае	пристапот до информации се ограничува според TLP ознаката, законските овластувања и оперативната потреба;
минимизација	се разменуваат само податоци неопходни за целта на постапувањето;
следливост	секоја класификација, промена, ескалација и размена мора да биде документирана;
усогласување со меѓународни стандарди	се применуваат признати стандарди кога тоа е соодветно и изводливо.

II. НАЦИОНАЛНА ТАКСОНОМИЈА НА ИНЦИДЕНТИ

Член 6
(Основа на таксономијата)

(1) Националната таксономија на сајбер безбедносни инциденти се заснова на ENISA Reference Security Incident Taxonomy (RSIT), со потребни национални приспособувања за секторите, органите и субјектите опфатени со Законот.

(2) MKD-CIRT ја одржува националната таксономија, ја објавува на својата интернет страница и ја ажурира по значајни измени на ENISA RSIT или по потреба утврдена од оперативната пракса.

(3) Сите тимови задолжително ја применуваат националната таксономија при документирање, размена, известување и агрегирање на податоци за инциденти.

Член 7
(Главни категории на инциденти)

Категорија	**Опис**
Abusive Content	Спам, злонамерна или незаконита содржина, злоупотреба на комуникациски канали и други форми на недозволена содржина.
Malicious Code	Злонамерен софтвер, ransomware, wiper, botnet, backdoor, тројанци, црви, cryptominer и слични појави.

Information Gathering	Скенирање, прибирање информации, sniffing, social engineering, phishing и други подготвителни активности.
Intrusion Attempts	Обиди за неовластен пристап, brute force, exploit attempts и искористување ранливости без потврден успешен пробив.
Intrusions	Успешен неовластен пристап, компромис на сметки, апликации, системи или мрежи.
Availability	DoS/DDoS, sabotage, outage, прекин или значајна деградација на услуга.
Information Content Security	Неовластен пристап, измена, губење, протекување или компромис на податоци.
Fraud	Измама, кражба на идентитет, злоупотреба на ресурси или акредитиви.
Vulnerable	Откриени ранливи, погрешно конфигурирани или изложени системи без потврдена експлоатација.
Other / Test	Инциденти кои не се вклопуваат во претходните категории, односно тест-записи кои јасно се означуваат како тест.

Член 8

(Подкатегории и минимално ниво на деталност)

(1) Секоја главна категорија се разложува во подкатегории согласно националниот каталог на подкатегории, кој MKD-CIRT го објавува како Анекс А.

(2) При документирање на инцидент, тимот го применува најниското ниво на подкатегоризација што може разумно да се утврди врз основа на достапните информации.

(3) Кога податоците се недоволни, се користи најблиската повисока категорија, а записот се ажурира веднаш по добивањето дополнителни факти.

Член 9

(Мапирање со MITRE ATT&CK)

(1) За значајни инциденти и за инциденти со меѓутимско или прекугранично влијание, тимовите вршат мапирање на тактики, техники и, кога е применливо, подтехники според MITRE ATT&CK.

(2) Се применува матрицата што одговара на засегнатата средина: Enterprise, ICS, Mobile или Cloud.

(3) Мапирањето се внесува во оперативната евиденција и во размената на информации кога тоа е соодветно и не ја нарушува доверливоста на изворот.

III. СЕРИОЗНОСТ, СТАТУС И МИНИМАЛНИ ПОЛИЊА

Член 10
(Петстепена скала на сериозност)

Ниво	Ознака	Опис
Критичен	C	Инцидент со национално, прекугранично или животозагрозувачко влијание, или со потенцијал за сајбер безбедносна криза.
Висок	H	Значајно нарушување кај суштински субјект, критична инфраструктура или услуга од висока критичност.
Среден	M	Нарушување кај важен субјект или ограничено влијание со можност за ескалација.
Низок	L	Локален инцидент со минимално влијание и без очигледен потенцијал за ескалација.
Информативен	I	Настан или наод со информативна вредност, без потврдено нарушување.

Член 11
(Димензии за оценување на сериозност)

Димензија	Опис
D1 — Оперативно влијание	траење, обем, обновливост и деградација на услугата;
D2 — Засегнати лица	број и тип на засегнати физички и правни лица;
D3 — Финансиско влијание	директни и индиректни загуби и трошоци;
D4 — Безбедност и здравје	потенцијал за повреди, загрозување живот или јавно здравје;
D5 — Доверливост и интегритет на податоци	обем и чувствителност на компромитираните податоци;
D6 — Географски опфат	локален, регионален, национален или прекуграничен опфат;
D7 — Каскадни ефекти	влијание врз други субјекти, сектори или услуги.

Член 12
(Статус на инцидент)

Статус	Значење
New	примен запис кој сè уште не е тријажиран;
Triaged	извршена првична проверка и класификација;
In Progress	инцидентот е во активна обработка;
Contained	ширењето е ограничено или спречено;
Eradicated	заканата е отстранета од засегнатите системи;
Recovered	услугата е обновена и валидирана;
Closed	завршено постапување и документирани поуки;
Reopened	записот е повторно отворен поради нови докази или повторна активност.

Член 13
(Минимални содржински елементи)

Секој тим, при размена или доставување запис за инцидент, најмалку ги користи следните групи на податоци: идентификатор, изворен тим, категорија и подкатегорија, сериозност, статус, TLP ознака, засегнат сектор и тип субјект, географски опфат, временски печати, краток опис, достапни IOC/TTP, преземени мерки и ограничувања за понатамошна дистрибуција.

Деталниот образец на минималните полиња се утврдува во Анекс Б, кој го одржува MKD-CIRT.

IV. TLP, ДОВЕРЛИВОСТ И ТЕХНИЧКИ ФОРМАТИ

Член 14
(Примена на TLP 2.0)

Ознака	Опсег на дистрибуција
TLP:RED	само за именувани приматели; без понатамошно дистрибуирање;
TLP:AMBER+STRICT	само во рамките на организацијата на примателот; без дистрибуција кон трети страни;
TLP:AMBER	во рамките на организацијата и кон директно засегнати клиенти или добавувачи на need-to-know основа;
TLP:GREEN	во рамките на заедница на доверба, но не јавно;
TLP:CLEAR	без ограничувања за дистрибуција.

TLP ознаките секогаш се користат во оригиналната англиска форма. Промена на TLP ознака е дозволена само со согласност на оригиналниот извор, освен кога изворот однапред определил поинакво правило.

Член 15
(Дополнителни ознаки)

Покрај TLP ознаката, информациите може да содржат ознака за доверба во изворот, ниво на аналитичка доверба, ограничување на употреба, секторска релевантност и, кога е применливо, ознака согласно прописите за класифицирани информации. Овие ознаки не ја заменуваат TLP ознаката, туку ја дополнуваат.

Член 16
(Формати за техничка размена)

Формат	**Намена**
STIX 2.1 / TAXII 2.1	структурирана и автоматизирана размена на CTI, IOC, TTP и кампањи;
MISP JSON	оперативна размена преку MISP инстанци;
IODEF	размена на информации за инциденти меѓу CSIRT тимови, кога е потребна компатибилност;
Sigma / YARA	детекциони правила за SIEM и малвер анализа;
Snort / Suricata	IDS/IPS правила за мрежно откривање;
MITRE ATT&CK STIX	стандардизирано мапирање на TTP.

MKD-CIRT воспоставува и одржува национална MISP инфраструктура како препорачана платформа за оперативна размена. Тимовите кои користат други платформи обезбедуваат техничка меѓуоперабилност со националната MISP инфраструктура.

V. СТАНДАРДИЗИРАНИ ПРАКТИКИ ЗА СПРАВУВАЊЕ СО ИНЦИДЕНТИ

Член 17
(Заеднички фазен модел)

Фаза	**Содржина**
1. Подготовка	одржување капацитети, контакти, playbook-и, канали и алатки;
2. Детекција и прием	прием на пријава, автоматска детекција или проактивно идентификување;
3. Тријажа и класификација	проверка, категоризација, сериозност, TLP, статус и надлежност;
4. Спречување и координација	ограничување на ширење, ескалација, барања за помош и размена;

5. Отстранување и обновување	отстранување на причината, валидација, обновување на услуги;
6. Затворање и поуки	финално документирање, RCA, препораки и ажурирање на процедури.

Член 18

(Показатели за изведба)

Сите тимови следат заеднички показатели: MTTA, MTTT, MTTC, MTTE, MTTR, стапка на придржување кон законските рокови, број на ескалирани инциденти и број на инциденти со повторно отворање. Показателите се користат за подобрување на нивото на зрелост, а не како единствена основа за оценување на квалитетот на работата.

Член 19

(Интегритет на докази)

При собирање и обработка на дигитални докази, тимовите применуваат принципи на интегритет, автентичност, следливост и синџир на старателство. Доказите се хешираат со SHA-256 или посилен алгоритам, а сите активности врз доказите се документираат со временски печат и идентитет на лицето кое ја извршило активноста.

Член 20

(Меѓутимска ескалација)

Кога инцидентот опфаќа субјекти од надлежност на повеќе тимови, ескалацијата се врши преку Мрежата на тимови за одговор на компјутерски инциденти. За инциденти со голем опфат или со можност за сајбер безбедносна криза, ескалацијата се врши кон Тимот за координација согласно Законот.

VI. СТАНДАРДИ ЗА УПРАВУВАЊЕ СО САЈБЕР БЕЗБЕДНОСНИ КРИЗИ

Член 21

(Нивоа на координација)

Ниво	Опис
Ниво 1 — Тимско справување	инцидентот се справува од еден тим или од ограничен број тимови без потреба од национална координација;
Ниво 2 — Меѓутимска координација	инцидентот засега повеќе тимови, сектори или субјекти и бара координирано делување преку Мрежата;
Ниво 3 — Национална координација	инцидент со голем опфат или сајбер безбедносна криза која бара активирање на Тимот за координација.

Член 22

(Ситуациски извештаи и шаблони)

За време на меѓутимско или кризно справување се користат стандардизирани шаблони за ситуациски извештај (SitRep), статусно известување, барање за информации, барање за помош

и завршен извештај. Шаблоните ги обезбедува MKD-CIRT како Анекс В и сите тимови ги применуваат во иста структура.

Член 23

(Оперативни прирачници (Playbooks))

MKD-CIRT одржува национални оперативни прирачници (playbooks) за најмалку следните сценарија: ransomware кај критични услуги, DDoS со национално влијание, supply-chain compromise, компромис на доверлива услуга, инцидент во ICS/OT средина, компромис на идентитети со висок привилегиран пристап и хибридна закана. Оперативните прирачници се ажурираат најмалку еднаш годишно и се тестираат преку вежби.

VII. КООРДИНИРАНО ОТКРИВАЊЕ НА РАНЛИВОСТИ

Член 24

(Национална CVD рамка)

MKD-CIRT, согласно Законот, ја врши координативната улога за координирано откривање на ранливости кога ранливоста има национално, меѓусекторско, прекугранично или системско значење. Тимовите ги препраќаат до MKD-CIRT пријавите за ранливости што го надминуваат нивниот секторски или организациски опфат.

CVD постапувањето се усогласува со ISO/IEC 29147, ISO/IEC 30111, FIRST PSIRT Services Framework и релевантните ENISA насоки.

Член 25

(Основни чекори во CVD постапка)

Чекор	Содржина
Прием	прифаќање на пријава, вклучувајќи можност за анонимно или доверливо пријавување;
Валидација	техничка проверка дали ранливоста постои и дали е релевантна;
Координација	идентификување засегнати страни и посредување меѓу пријавителот и производителот/давателот;
Корекција	следење на изработка и тестирање на patch, workaround или компензациски мерки;
Обелоденување	координирано јавување на информацијата во договорен рок и со соодветна TLP ознака пред јавна објава;
Затворање	документирање на исходот, поуки и препораки.

Член 26

(Рокови за обелоденување)

Стандардниот рок за координирано објавување е 90 дена од потврда на валидноста на ранливоста. Рокот може да се скрати кога ранливоста активно се експлоатира или кога постои

висок јавен интерес, односно да се продолжи кога корекцијата е сложена и постои документирано образложение.

VIII. ОЦЕНУВАЊЕ НА РАНЛИВОСТИ

Член 27
(CVSS, EPSS и KEV)

За оценување на ранливости, тимовите применуваат CVSS како основна скала за сериозност, EPSS како дополнителен индикатор за веројатност на експлоатација и релевантни каталози на познато експлоатирани ранливости како извор за приоритизација. Кога MKD-CIRT издава национално советување за ранливост, во него ги наведува релевантните оценки, познатата експлоатација и препорачаните рокови за корекција.

Член 28
(Оперативни рокови за корекција)

Сериозност	Оперативна насока
Критична	итна корекција или компензациска мерка;
Висока	корекција во краток рок согласно ризикот и изложеноста;
Средна	корекција во редовен циклус со приоритетно следење;
Ниска	корекција во редовен циклус на одржување;
Информативна	документирање и следење без итна корекција.

IX. УСОГЛАСЕНОСТ, ПОДДРШКА И АЖУРИРАЊЕ

Член 29
(Известување за усогласеност)

Секој тим доставува до MKD-CIRT годишен извештај за усогласеност со националните шеми и практики, најдоцна до 28 февруари за претходната календарска година. Извештајот содржи степен на примена на таксономијата, скалата на сериозност, TLP, MITRE ATT&CK мапирање, форматите за размена и статусот на техничка интеграција.

Член 30
(Поддршка од MKD-CIRT)

MKD-CIRT обезбедува обуки, технички упатства, шаблони, речници, консултативна поддршка и координативни состаноци за сите тимови. Координативни состаноци за усогласување се одржуваат најмалку еднаш во шест месеци.

Член 31
(Преиспитување и ажурирање)

Овој правилник се преиспитува најмалку еднаш во две години, како и по значајни промени на релевантните стандарди, Законот или оперативната пракса. Предлог-измените ги подготвува MKD-CIRT во консултација со Мрежата на тимови за одговор на компјутерски инциденти, а ги усвојува директорот на Агенцијата.

X. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 32
(Преодни рокови)

(1) Тимовите ја применуваат националната таксономија и петстепената скала на сериозност во рок од шест месеци од денот на влегувањето во сила на овој правилник.

(2) Мапирањето со MITRE ATT&CK за значајни инциденти се применува во рок од девет месеци.

(3) Техничката интеграција со националната MISP инфраструктура или еквивалентна меѓуоперабилна размена се воспоставува во рок од дванаесет месеци.

(4) До истекот на преодните рокови, постојните практики се применуваат во делот во кој не се спротивни на овој правилник.

Член 33
(Анекси)

MKD-CIRT во рок од 90 дена од денот на влегувањето во сила ги објавува и одржува следните анекси: Анекс А — каталог на подкатегории; Анекс Б — минимални полиња на запис за инцидент; Анекс В — шаблони за ситуациски и меѓутимски комуникации; Анекс Г — национален CVD шаблон; Анекс Д — македонско-англиски речник на оперативна терминологија.

Член 34
(Однос со други акти)

Овој правилник се применува паралелно со правилниците и методологиите за пријава и постапување по инциденти, евиденција на инциденти, Национален регистар на сајбер инциденти, прагови за значајни инциденти и размена на информации. Во случај на неусогласеност со внатрешни процедури на тим, предимство има заедничката национална шема утврдена со овој правилник, освен ако со посебен закон не е определено поинаку.

Член 35
(Влегување во сила)

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

Бр. 0101-1513/20
14.07. 2026 година
Скопје

Директор
на Агенцијата за електронски комуникации
Nusret Haliti

Изготвил:
Раководител на MKD-CIRT
Sevdali Selmani