Врз основа на член 37 став (6) 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 (8), член 37 ставови (1), (2), (3), (4) и (5) и член 61 став (1) од истиот закон, директорот на Агенцијата за електронски комуникации донесе

ПРАВИЛНИК

за начинот на размена на податоци и информации за сајбер безбедност помеѓу суштинските и важните субјекти од надлежност на Агенцијата за електронски комуникации преку MKD-CIRT и, кога е релевантно, со нивните добавувачи или даватели на услуги

I. ОПШТИ ОДРЕДБИ

Член 1

(Предмет)

Со овој правилник се уредуваат начинот на размена на податоци и информации за сајбер безбедност, како и процедурите за нивна размена, за областите и субјектите од надлежност на Агенцијата за електронски комуникации преку Националниот центар за одговор на компјутерски инциденти — MKD-CIRT.

Правилникот се однесува на доброволна размена на релевантни информации помеѓу суштинските и важните субјекти, помеѓу тие субјекти и нивните добавувачи или даватели на услуги, како и помеѓу субјектите и MKD-CIRT, кога таквата размена е потребна за спречување, откривање, одговор, обновување или ублажување на сајбер безбедносни ризици и инциденти.

Член 2

(Правна природа и ограничување на примената)

Размената уредена со овој правилник е доброволна и не претставува замена за задолжителните обврски за известување за значајни сајбер безбедносни инциденти согласно Законот. Ако споделената информација укажува на значаен инцидент, се применуваат правилата за пријавување и постапување по инциденти.

Овој правилник не ја уредува размената на класифицирани информации, комуникацијата со органите од областа на безбедноста, одбраната и гонењето на сторителите на кривични дела, ниту комерцијалната продажба на разузнавачки информации за закани. Тие прашања се уредуваат со посебни прописи, протоколи или договори.

Член 3

(Начела)

Размената на информации се врши законито, целно, доброволно, пропорционално и навремено. Секој учесник обезбедува информациите да се обработуваат само за сајбер безбедносни цели, со почитување на принципите на минимизација, доверливост, интегритет, „потреба да се знае", следливост и заштита на изворот.

Кога информациите се добиени од друг субјект, нивното понатамошно споделување се врши само во рамките на дозволената ознака за дистрибуција и во согласност со условите поставени од изворот.

Член 4

(Опфат на информациите)

Размената може да опфати технички, оперативни, тактички и стратешки информации релевантни за сајбер безбедноста. За полесна примена, информациите се групираат во следните категории:

Категорија	Примери на информации
Закани и кампањи	Информации за сајбер закани, заканувари, кампањи, мотивации, капацитети и очекувани цели.
Ранливости и изложеност	Информации за ранливости, погрешни конфигурации, изложени услуги, достапни експлоити и препораки за санација.
Индикатори и правила за детекција	IP адреси, домени, URL, hash вредности, YARA/Sigma/Snort/Suricata правила, IoC и IoA.
Тактики, техники и процедури	TTP информации, мапирање со MITRE ATT&CK, модели на напад и начини на движење во инфраструктура.
Предупредувања и препораки	Сајбер безбедносни предупредувања, конфигурациски насоки, hardening препораки и оперативни совети.
Искуства и анализи	Извештаи од анализа на инциденти, научени поуки, анонимизирани случаи и трендови.

Член 5

(Цели на размената)

Размената мора да има јасна сајбер безбедносна цел. Таа може да служи за спречување и откривање на инциденти, ограничување на нивното ширење, координиран одговор, обновување на услугите, отстранување на ранливости, подобрување на одбранбените способности и развој на заеднички техники за откривање и ублажување на закани.

Информациите не смеат да се користат за конкурентски, комерцијално чувствителни, дискриминаторни или други цели кои не се поврзани со сајбер безбедност.

II. МЕХАНИЗМИ, АЛАТКИ И ОЗНАЧУВАЊЕ

Член 6

(Механизми за размена)

Размената се врши преку однапред определени и безбедни механизми. MKD-CIRT може да координира национални, секторски или ад хок механизми за размена, зависно од природата на информациите, нивната чувствителност и оперативната итност.

Механизам	Намена
Безбедна електронска комуникација	Размена на ограничени информации помеѓу познати и проверени точки за контакт.
Единствен портал за сајбер безбедност	Користење кога технички е овозможено и согласно начинот на пристап и користење пропишан од министерот.
MISP или еквивалентна платформа	Структурирана размена на индикатори, предупредувања, атрибути и технички правила во доверливи заедници.
Секторски механизми / ISAC	Размена во рамки на сектор со заеднички ризици и меѓузависности.

Билатерални или регионални канали	Координација со партнерски CSIRT тимови и меѓународни партнери, во рамки на применливите договори.

Член 7

(Усогласување со единствениот портал)

Техничките канали и процедурите за размена се препорачува да се усогласат со правилникот за начинот на пристап и користење на единствениот портал за сајбер безбедност од член 15 став (8) од Законот, кога тој ќе биде донесен и кога порталот ќе биде оперативно достапен за оваа намена.

До целосната оперативна употреба на порталот, размената се врши преку безбедни канали определени од MKD-CIRT. Таквото привремено постапување не ја ограничува обврската за подоцнежно техничко усогласување со порталот.

Член 8

(Технички формати и алатки)

За структурирана и машински обработлива размена се користат меѓународно прифатени формати и алатки, со предност на решенија кои овозможуваат проверливост, автоматизација, контрола на пристап и следливост.

Тип	Препорачана примена
STIX/TAXII	Структурирана размена на закани, индикатори, кампањи и TTP информации.
MISP JSON	Оперативна размена на индикатори и предупредувања во доверливи заедници.
IODEF/RID	Координација помеѓу тимови за одговор на компјутерски инциденти.
Sigma, YARA, Snort/Suricata	Размена на правила за детекција, анализа на злонамерен софтвер и IDS/IPS употреба.
PGP/S-MIME и TLS	Заштита на доверливоста, автентичноста и интегритетот на комуникацијата.

Член 9

(Означување и чувствителност)

Секоја информација што се споделува мора да има јасно означен режим на дистрибуција. Како основен модел се користи Traffic Light Protocol (TLP), а кога информацијата содржи лични податоци, деловна тајна, безбедносно чувствителни информации или класифицирани информации, се применуваат и соодветните прописи.

Ознака	Основно правило
TLP:RED	Само за именувани приматели; без понатамошно дистрибуирање.
TLP:AMBER+STRICT	Само во организацијата на примателот; без споделување со трети страни.
TLP:AMBER	Во организацијата и со директно засегнати партнери на need-to-know основа.
TLP:GREEN	Во заедницата на доверба; не за јавност.
TLP:CLEAR	Информација погодна за јавна или поширока дистрибуција.

Промена на TLP ознаката се врши само со согласност на изворот или согласно правилата на механизмот за размена.

Член 10

(Заштита на лични податоци, деловна тајна и класифицирани информации)

Кога информацијата содржи лични податоци, се споделуваат само оние податоци кои се неопходни за сајбер безбедносната цел. Каде што е можно, се применува анонимизација, псевдонимизација или агрегација. Личните податоци се обработуваат согласно прописите за заштита на личните податоци.

Информации кои претставуваат деловна тајна, безбедносно чувствителна содржина или класифицирана информација се споделуваат само преку соодветен канал и со применливо ниво на заштита. Овој правилник не претставува правен основ за откривање класифицирани информации надвор од режимот утврден со посебните прописи.

III. ПОСТАПКА ЗА РАЗМЕНА

Член 11

(Учесници и точки за контакт)

Секој субјект кој учествува во механизам за размена назначува точка за контакт за сајбер безбедност и обезбедува валидни контакт податоци, безбеден комуникациски канал и лице овластено да одобрува или прима информации со ограничена дистрибуција.

MKD-CIRT води евиденција на учесници во механизмите што ги координира, со податоци за субјектот, контакт точката, каналот за комуникација, датумот на пристапување и евентуалното повлекување од механизмот.

Член 12

(Кодекс на однесување)

За учество во механизам координиран од MKD-CIRT, учесникот прифаќа Кодекс на однесување. Кодексот ги уредува доверливоста, почитувањето на TLP ознаките, забраната за неовластено понатамошно дистрибуирање, заштитата на изворот, правилата за конкуренција, одговорноста за точност на информациите и последиците од повреда на правилата.

Кодексот на однесување се донесува како оперативен документ на MKD-CIRT и се објавува заедно со техничките насоки за пристап до механизмот.

Член 13

(Пуштање и прием на информации)

Пред споделување, изворот ја проверува релевантноста, точноста и чувствителноста на информацијата, определува TLP ознака и го избира соодветниот канал. Кога постои активен напад или непосредна закана, споделувањето може да се изврши забрзано, со последователно дополнување на метаподатоците и документацијата.

Примателот ја проверува автентичноста и интегритетот на добиената информација, ја почитува ознаката за дистрибуција, ја обработува според сопствената безбедносна потреба и, кога е соодветно, доставува повратна информација до изворот или до MKD-CIRT за нејзината оперативна корисност.

Член 14

(Добавувачи и даватели на услуги)

Размена со добавувачи или даватели на услуги се врши кога тие се релевантни за спречување, откривање, одговор или ублажување на сајбер безбедносен ризик. Субјектот обезбедува таквата размена да биде покриена со договорни клаузули за доверливост, ограничена употреба, безбедна обработка, известување за повреда на доверливоста и враќање или бришење на информации по завршување на потребата.

Добавувачот или давателот на услуга не смее да ја користи добиената информација за друга цел и не смее да ја пренесува на трети лица без претходна согласност на изворот, освен кога таквото пренесување е неопходно и законски дозволено.

Член 15

(Секторски механизми и ISAC)

MKD-CIRT може да поддржи воспоставување секторски механизми за размена, вклучително и информациски заеднички центри (ISAC), кога субјектите имаат споредлив закановен пејзаж, меѓузависни услуги или заеднички потреби за координирана одбрана.

Секторскиот механизам се уредува со меморандум, кодекс или друг писмен документ кој ги опишува целите, членството, каналите за размена, правилата за доверливост, начинот на координација со MKD-CIRT и постапката за влез и излез на учесници.

Член 16

(Известување до Министерството)

Суштинските и важните субјекти го известуваат Министерството за дигитална трансформација за учество во механизам за споделување информации и за повлекување од таков механизам, согласно Законот. Известувањето може да се достави преку MKD-CIRT како надлежен орган за субјектите од негова надлежност.

Кога единствениот портал за сајбер безбедност ќе биде оперативно достапен за оваа намена, известувањата се доставуваат преку порталот. До тогаш, известувањето се доставува преку безбеден канал определен од MKD-CIRT.

Член 17

(Применливост на член 37 став (5))

Одредбите кои се однесуваат на помошта на Министерството за дигитална трансформација во воспоставување механизми за споделување информации, со примена на најдобри практики на Европската унија и НАТО, се применуваат од денот на пристапувањето на Република Северна Македонија во Европската унија, согласно член 61 став (1) од Законот.

До тој ден, MKD-CIRT може да дава стручна и техничка поддршка за воспоставување механизми за размена во рамките на своите законски надлежности и расположливи капацитети.

IV. ЗАШТИТА, ЕВИДЕНТИРАЊЕ И ПРЕОДНИ ОДРЕДБИ

Член 18

(Евидентирање, следливост и квалитет)

MKD-CIRT и учесниците во механизмите за размена обезбедуваат евидентирање на релевантните дејствија поврзани со споделување, прием, пристап, измена, извоз и бришење на информации. Евиденцијата треба да овозможи проверка на изворот, времето на размена, ознаката за дистрибуција и опсегот на примателите.

MKD-CIRT може периодично да го оценува квалитетот на размената преку агрегирани показатели, како број на активни учесници, број на споделени информации, навременост, корисност на индикаторите и број на спречени или ублажени закани. Објавувањето на такви показатели се врши само во агрегирана и анонимизирана форма.

Член 19

(Преодни одредби)

MKD-CIRT во рок од 90 дена од денот на влегувањето во сила на овој правилник подготвува образец за известување за учество во механизам за размена, образец за назначување точка за контакт и предлог Кодекс на однесување.

Постојните неформални механизми за размена на информации се усогласуваат со овој правилник во рок од 12 месеци. До нивното усогласување, тие може да продолжат да функционираат ако не се во спротивност со Законот, TLP правилата и прописите за заштита на лични податоци и класифицирани информации.

Член 20

(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. 0101-1513/19

14.07. 2026 година

Скопје

Директор

на Агенцијата за електронски комуникации

Nusret Haliti

Изготвил:

Раководител на MKD-CIRT
Sevdali Selmani