Република Северна Македонија

Министерство за дигитална трансформација

ПОЛИТИКА ЗА ОТКРИВАЊЕ НА ИНФОРМАЦИИ (Traffic Light Protocol-TLP)

Министерство
за дигитална трансформација на
Република Северна Македонија

Ул. „Филип Втори Македонски" бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk

СОДРЖИНА:

Ул. „Филип Втори Македонски" бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk

1.Вовед

Обработката на осетливи информации претставува суштински аспект во секојдневното работење на Тим за одговор на компјутерски инциденти за органите на извршната власт - MKD-GOV-CSIRT, кој функционира во рамки на Министерството за дигитална трансформација. Осетливи информации можат да бидат доставени до MKD-GOV-CSIRT преку пријави на сајбер безбедносни инциденти од страна на органите на државната управа, институции, како и од други релевантни страни вклучени во процесите за управување со сајбер безбедносни инциденти и закани. MKD-GOV-CSIRT ја применува рамката Traffic Light Protocol (TLP) Version 2.0 во согласност со упатствата на FIRST (Forum of Incident Response and Security Teams) за контролирано споделување на информации.

Одржувањето на довербата во способноста на MKD-GOV-CSIRT за соодветна заштита, ракување и контролирано споделување на осетливи информации е од суштинско значење за ефективно извршување на неговите законски надлежности. Во таа насока, правилата за откривање и споделување на информации опишани во овој документ имаат за цел да обезбедат јасни насоки и принципи за одржување на високо ниво на доверливост, интегритет и доверба во работењето на MKD-GOV-CSIRT.

1.1Цел

Целта на оваа политика е да ги дефинира и опише принципите, правилата и ограничувањата кои MKD-GOV-CSIRT ги применува при откривање, објава и споделување на информации во рамки на своето работење.

Оваа политика, заедно со Политиката за класификација на информациите на MKD-GOV-CSIRT, претставува составен дел од рамката за управување со информации и има за цел обезбедување на доверливоста, интегритетот и достапноста на податоците со кои располага MKD-GOV-CSIRT.

1.2Опсег

Оваа политика се применува на сите информации и информациски средства кои се создадени, примени, обработувани, управувани, складирани, пренесувани или на друг начин евидентирани од страна на MKD-GOV-CSIRT, без оглед на нивната форма или медиум.

Политиката е задолжителна за сите вработени, ангажирани лица и други субјекти кои, врз основа на закон, овластување, договор или воспоставена соработка, имаат пристап до информации обработувани од MKD-GOV-CSIRT.

1.3Врски и референци

- **Закони**
    - Закон за безбедност на мрежни и информациски системи

Министерство
за дигитална трансформација на
Република Северна Македонија

Ул. „Филип Втори Македонски" бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk

- Закон за заштита на личните податоци
- Закон за електронски комуникации
- Закон за класифицирани информации

- **Внатрешни политики и образци на MKD-GOV-CSIRT**
  - Политика за класификација на информации
  - Образец: Овластување за откривање на информации
  - Образец: Договор за неоткривање на информации (NDA)

- **Меѓународни упатства и стандарди за TLP 2.0**
  - FIRST.org – Traffic Light Protocol (TLP)
  - CISA – TLP 2.0 User Guide
  - CERT-EU Blog – TLP Version 2 Primer

2. Дефиниции

2.1. Информациска размена

Информациска размена е пренос или споделување на информации меѓу MKD-GOV-CSIRT, неговите конституенти и други релевантни страни. Ова може да се случува:

- Лично, на состаноци на CSIRT тимови или со конституенти на MKD-GOV-CSIRT;
- На состаноци на кои учествуваат стручни лица за сајбер безбедност;
- Електронски, преку е-пошта, безбедни платформи или телефонски повици.

2.2. Анонимизација

Анонимизација е процес на бришење или замена на идентификациски информации за поединци или организации, со цел да се заштити приватноста и доверливоста на податоците при нивно споделување.

3. Одговорност за управување со податоци

Сите членови на MKD-GOV-CSIRT имаат обврска да ја заштитат доверливоста на податоците со кои работат, без оглед на формата или медиумот на кој податокот е запишан или преку кој се пренесува, согласно процедурите за работа на MKD-GOV-CSIRT.

MKD-GOV-CSIRT е одговорен за имплементација на соодветни процедурални, физички и технички контроли за пристап, користење, пренос или депонирање на податоците што се во сопственост на или ги користи MKD-GOV-CSIRT, во согласност со оваа политика.

Со цел да се избегне каква било протекување на осетливи информации, членовите на MKD-GOV-CSIRT ќе откриваат информации само ако е неопходно и во согласност со правилата дефинирани во оваа политика.

Министерство
за дигитална трансформација на
Република Северна Македонија

Ул. „Филип Втори Македонски" бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk

4. Откривање на информации

4.1. Заштита на информации

При размена на информации, **MKD-GOV-CSIRT** го применува принципот „потребно е да знае“ (*need-to-know*):

- Информацијата што не е јавна **не смее** да се споделува јавно и **мора** да се сподели само со оние субјекти што треба да ја знаат,
- Откривањето и споделувањето на информацијата ќе се врши во согласност со **оригиналното ниво на доверливост**,
- **MKD-GOV-CSIRT** ја почитува класификацијата на информацијата доделена од страна на изворот што ја доставил информацијата, согласно процедурите за внатрешно работење,
- Откривање и објава на осетливи информации се врши **само ако е неопходно** за решавање на инцидентот. Принципите за анонимизација на податоците се наведени во точка 4.4.

4.2. Соработка со други страни

MKD-GOV-CSIRT често соработува со други CSIRT тимови, засегнати страни, производители, добавувачи и извршни органи на власта.
Откривањето на информации на овие групи се врши **поединечно и сразмерно со ризикот** од откривање на информацијата.
Пред откривање на информации, **MKD-GOV-CSIRT** може да побара потпишување на **Договор за неоткривање на информации (NDA)**.
Чесноста и доверливоста на партнерите се проверува пред размена на доверливи информации.

4.3. Безбедност при комуникација:

Секогаш кога се прави информацијата достапна за други:

- таа мора да биде **потпишана**, за да се обезбеди неотповикливост;
- таа мора да биде **шифрирана**, за заштита на доверливоста, секогаш кога е потребно согласно оваа политика.

4.4. Заштита на лични податоци и правни аспекти

MKD-GOV-CSIRT ги доставува бараните информации на државни органи, јавни институции или овластени трети страни само кога постои законска обврска за тоа. Ова значи дека секоја достава се врши по исполнување на сите релевантни законски барања, на пример, преку доставување на судски налог или друг официјален акт, со цел да се обезбеди легитимност и правна заштита на процесот.

Секој случај на обработка или пренос на лични податоци според форма и содржина ќе биде во согласност со Законот за заштита на личните податоци, Законот за класифицирани информации, Законот за електронски комуникации и другите важечки прописи во Република Северна Македонија, при тоа имајќи ги предвид политиките и одлуките за класификација на информации на НАТО и Европската Унија.

Министерство
за дигитална трансформација на
Република Северна Македонија

Ул. „Филип Втори Македонски” бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk

4.5. Анонимизација

Според дефиницијата од точка 2.2 пред да се споделат со трета страна, осетливите информации секогаш ќе се анонимизираат. Ова значи дека лични податоци или други податоци со кои може да се идентификуваат субјекти или цели на компјутерски напад не се разменуваат, освен ако не е обезбедена експлицитна писмена согласност на сопственикот на податоците или доколку податоците се соодветно анонимизирани.
Размена на информации со трети страни се врши само кога е неопходно за решавање на инцидент.

Во случаи кога анонимизацијата не е практична или е контрапродуктивна за справување со инцидентот, MKD-GOV-CSIRT го задржува правото да сподели не-анонимизирани информации само со групи или трети лица со кои е изградено доверлив однос.

Сите вакви размени се извршуваат во согласност со важечките закони на Република Северна Македонија, како и со експлицитно писмено одобрување од страна на сопственикот на информацијата што се разменува (користејќи Образец – Овластување за откривање на информација – Authorization to Disclose Information).

4.6. Користење на TLP за споделување на информации

4.6.1. Општи принципи

За да ги заштити информациите што ги обработува и споделува, MKD-GOV-CSIRT ќе ја применува и својата Политика за класификација на информации заедно со Traffic Light Protocol (TLP) како рамка за контролирано споделување.

При размена на информации, MKD-GOV-CSIRT ќе ги означи информациите со соодветна TLP ознака само со страни што го прифатиле користењето на TLP. Ако страната со која се разменува информацијата не применува TLP протокол, MKD-GOV-CSIRT ќе иницира проверка и усогласување на употребените нивоа на доверливост помеѓу двете страни пред да се сподели информација.

Правилата и општите принципи на TLP се дадени во Прилог – Користење на TLP (Traffic Light Protocol) за споделување на информации и се дел од оваа политика.

Секоја комуникација или размена на информации со ниво повисоко од TLP:GREEN, вклучително и пораки по електронска пошта или документи, мора да биде означена со ознаката „[TLP: Боја]“, каде Боја може да биде RED, AMBER+STRICT, AMBER, GREEN или CLEAR. Слична ознака или печат треба да биде јасно видлива на почетокот на пораката или на корицата/заглавието на документот што го испраќа или објавува MKD-GOV-CSIRT.

Доколку комуникацијата се врши усно, на пример преку телефонски разговор или видео конференција, соодветното TLP ниво треба јасно да се наведе на почетокот од разговорот, пред да се открие каква било информација.

Министерство
за дигитална трансформација на
Република Северна Македонија

Ул. „Филип Втори Македонски” бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk

4.6.2. Стандардно TLP ниво на класификација

Како почетно ниво MKD-GOV-CSIRT може да користи TLP:AMBER, но конечната класификација на информацијата се утврдува врз основа на проценка на ризик, контекстот на инцидентот и насоките на FIRST TLP 2.0.

Анекс 1 – Користење на TLP (Traffic Light Protocol) за споделување на информации

Секоја информација што се разменува од страна на MKD-GOV-CSIRT мора задолжително да биде означена со соодветна TLP ознака според следната табела. Ако информацијата што се разменува не е претходно означена од изворот, MKD-GOV-CSIRT ќе ја означи автоматски со TLP:AMBER.

ОЗНАКА	ОБЈАСНУВАЊЕ ЗА КОРИСТЕЊЕ
TLP RED	ИНФОРМАЦИЈА ШТО НЕ СЕ ОТКРИВА и е ограничена само на претставници на учесниците во размената на информацијата. Претставниците не смеат да ја споделуваат информацијата надвор од учесниците на размената на оваа информација. За информација означена со ниво TLP RED може да се дискутира само за време на размената на оваа информација, кога сите учесници на размената на информацијата се согласни за тоа. Лица или страни кои не се учесници во размената на TLP RED информација НЕ СМЕАТ да присуствуваат на размената или дискусијата по информацијата.
TLP AMBER	ИНФОРМАЦИЈАТА ИМА ОГРАНИЧЕНО ОТКРИВАЊЕ и е наменета само за членовите на информацискатa размена: членови на организации или конституенти (директно вработени лица, консултанти, или други ангажирани работници) кои го исполнуваат условот „ПОТРЕБНО Е ДА ЗНАЕ“ со цел да можат да постапат по информацијата.
TLP AMBER+STRICT	ИНФОРМАЦИЈАТА ИМА ОГРАНИЧЕНО ОТКРИВАЊЕ и е наменета само за членови на својата организација или конституентот кои треба да знаат за да можат да постапат по информацијата. Може да се споделува само внатре во организацијата и само со оние што го исполнуваат принципот „потребно е да знае“, со цел заштита на организацијата и спречување на понатамошна штета.
TLP GREEN	ИНФОРМАЦИЈАТА МОЖЕ ДА СЕ СПОДЕЛУВА СО ДРУГИ ОРГАНИЗАЦИИ, при информациска размена со индивидуи и експерти во областа на информацискатa безбедност, но не смее да се објавува јавно и поставува на јавна веб-страница.

Министерство
за дигитална трансформација на
Република Северна Македонија

Ул. „Филип Втори Македонски” бр.11, Скопје
Република Северна Македонија

+389 2 320 0999
www.mdt.gov.mk

TLP CLEAR	ЈАВНА ИНФОРМАЦИЈА, нема ограничување во нејзината дисеминација, објава, поставување на јавни веб-страници или емитување. Секој член на Информациската размена може да ја објави информацијата со почитување на правата за заштита на интелектуална сопственост.

Анекс 2 – Размена на информации

Ниво / Контакт	Разменувани информации	Одговорно лице	Складирање / техничка обработка	Ниво на дистрибуција
Внатрешно–организација	Податоци за тимот, стандардни оперативни процедури (SOPs), планирање на смени и внатрешни контакти	Раководител на сектор за сајбер безбедност + Раководител на одделение за подготовка и координација на политики за сајбер безбедност	RTIR (систем за управување со инциденти) / SIEM (систем за управување со безбедносни информации и настани) / MIOShare (платформа за размена на информации)	Внатрешно

Национално – други институции и конституенти	Известувања за инциденти, тактики, техники и процедури (TTPs), извештаи, аларми и засегнати системи	Советник за безбедност на мрежни и информациски системи во Министерството + Советник за безбедност на мрежни и информациски системи во други институции од јавниот сектор	RTIR (систем за управување со инциденти) / SIEM (систем за управување со безбедносни информации и настани) / MIOShare (платформа за размена на информации)	Ограничено (на ниво на конституенти и партнерски институции)
Меѓународно – други CSIRT тимови (FIRST, регионални CSIRT тимови), меѓународни партнери	Индикатори на компромитација (IOCs), извештаи за закани, тактики, техники и процедури (TTPs), аларми, покани за состаноци и известувања	Помлад соработник за меѓународни комуникации + Советник за подготовка на прописи од областа на сајбер безбедноста + Советник за безбедност на мрежни и информациски системи во Министерството	RTIR / MIOShare / безбедносна електронска пошта	Ограничено/ доверливо за меѓународни партнери