Република Северна Македонија

Министерство за дигитална трансформација

ПОЛИТИКА ЗА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

1.Вовед

Ефективното функционирање на јавните институции се заснова на континуирана обработка, размена и складирање на значителен обем на информации, од кои одреден дел имаат чувствителен или класифициран карактер. Неовластениот пристап, откривање или злоупотреба на ваквите информации може да предизвика сериозни последици врз институционалното работење, правниот поредок и националната безбедност.

Врз основа на Уставот на Република Северна Македонија и Законот за класифицирани информации, Министерството за дигитална трансформација ја донесува оваа Политика за класифицирани информации.

Со оваа политика се воспоставува стратешка и управувачка рамка за класификација, управување, заштита и контролирано споделување на информациите во текот на целиот нивен животен циклус.

Политиката е усогласена со националното законодавство, како и со меѓународно признатите стандарди и најдобри практики во областа на информацискатa безбедност, вклучително:

- ISO/IEC 27001 и ISO/IEC 27002
- Насоките на FIRST Traffic Light Protocol (TLP)
- SIM3 моделот за зрелост на безбедносни операции

Целта на оваа политика е обезбедување на регулаторна усогласеност и воспоставување конзистентен, ризично базиран и стандардизиран пристап за заштита на класифицираните и чувствителните информации.

2.Цел

Целта на оваа политика е да воспостави јасни, структурирани и законски усогласени правила за класификација, означување, користење, споделување и заштита на сите информации со кои ракува Министерството за дигитална трансформација.

Со оваа политика се настојува да се:

- обезбеди заштита на класифицираните и чувствителните информации;
- намали ризикот од неовластен пристап, откривање, губење или злоупотреба на информации;

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

- обезбеди усогласеност со Законот за класифицирани информации и поврзаните прописи;
- воспостави јасна контрола на пристап врз основа на принципот „потреба да се знае“;
- овозможи безбедно и контролирано споделување на информации преку Traffic Light Protocol (TLP);
- обезбеди конзистентен пристап кон управувањето со информации базиран на нивниот животен циклус;
- ја зајакне свесноста и одговорноста на вработените и партнерите во однос на заштитата на информациите.

3.Опсег

Оваа политика се применува на сите информации поврзани со субјектите на MKD-GOV-CSIRT кои се создаваат, примаат, обработуваат, складираат или споделуваат од страна на Министерството за дигитална трансформација, без оглед на нивната форма, формат или медиум. Политиката ги опфаќа следните категории:

Информации

- Сите документи во хартиена форма
- Електронски документи, бази на податоци и системи за обработка на информации
- Е-пошта, службена кореспонденција и комуникации
- Аудио, видео и мултимедијални записи
- Работни материјали, извештаи, анализи и службени белешки

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

Лица

- Вработени во Министерството за дигитална трансформација
- Договорни извршители и соработници
- Добавувачи и надворешни партнери
- Трети лица на кои им е одобрен пристап до информации

Процеси

- Создавање, прием и обработка на информации
- Складирање и чување на информации
- Споделување и пренос на информации
- Архивирање и уништување
- Контрола на пристап и ракување со информации во согласност со нивоата на класификација и TLP-ознаките.

4. Дефиниции

Овој дел ги утврдува клучните поими и концепти што се користат во политиката за класификација на информации, со цел обезбедување на конзистентно и заедничко разбирање на мерките и постапките за класификација, ракување и заштита на информациите.

1. Информација
Информација претставува знаење кое може да се комуницира во која било форма, вклучително записи, податоци, документи или комуникации што се создаваат, примаат, складираат или споделуваат од страна на Министерството за дигитална трансформација, без оглед на форматот (хартиен, електронски или дигитален).

2. Информации од значење за Република Северна Македонија
Информации од значење за Република Северна Македонија се информации класифицирани согласно нивото на чувствителност и потребата од заштита, при што пристапот до нив е ограничен исклучиво на овластени лица.

3. Класифицирани информации
Класифицирани информации се информации кои:

- се однесуваат на јавната безбедност, одбраната, надворешните работи или разузнавачките и безбедносните активности;
- спаѓаат во делокругот на работа на државните органи, органите на локалната самоуправа или правните лица основани од државата;
- мора да бидат заштитени од неовластен пристап и се означени со соодветно ниво на класификација.

4. Принцип „потреба да се знае“

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

Принципот „потреба да се знае“ обезбедува дека пристап до класифицирани информации им се доделува исклучиво на лица кои:

- поседуваат соодветен безбедносен сертификат; и
- имаат оправдана оперативна потреба за пристап до информацијата заради извршување на своите работни задачи или надлежности.

5. Ракување со класифицирани информации

Ракувањето со класифицирани информации го опфаќа целокупното управување со нивниот животен циклус, вклучувајќи:

- создавање и прием;
- евидентирање и означување;
- користење и обработка;
- пренос и споделување;
- архивирање;
- прекласификација или декласификација;
- безбедно уништување.

Сите активности се извршуваат во согласност со правилата за класификација и примената на TLP-ознаките.

5.Traffic Light Protocol (TLP)

Покрај националниот систем за класификација, Министерството за дигитална трансформација го применува и Traffic Light Protocol (TLP) како оперативен механизам за контролирано споделување на чувствителни информации.

TLP обезбедува практична рамка за:

- ограничување на дистрибуцијата на информации;
- овозможување контролирано споделување на информации со партнери;
- намалување на ризикот од компромитирање на информации;
- поддршка на соработката во областа на сајбер-безбедноста.

Примената и ракувањето со TLP-ознаките се врши во согласност со Политиката на Министерството за дигитална трансформација за објавување и споделување на информации (TLP), изработена во согласност со стандардите на FIRST TLP.

6. Нивоа на класификација

Министерството за дигитална трансформација го применува националниот систем за класификација на информации. Нивото на класификација го утврдува создавачот на

информацијата или овластено лице, врз основа на содржината и потенцијалното влијание од неовластено откривање.

Информациите се класифицираат во следните нивоа:

ДРЖАВНА ТАЈНА
• Неовластено откривање би предизвикало непоправлива штета врз трајните интереси на Република Северна Македонија.

СТРОГО ДОВЕРЛИВО
• Неовластено откривање би предизвикало исклучително сериозна штета врз виталните интереси на државата.

ДОВЕРЛИВО
• Неовластено откривање би предизвикало сериозна штета врз значајните интереси на државата.

ИНТЕРНО
• Неовластено откривање би предизвикало штета врз работењето на институциите и правните лица релевантни за јавната безбедност, одбраната, надворешните работи, како и разузнавачките и безбедносните активности.

Административна безбедност

Административната безбедност ги воспоставува управувачките процеси за класификација, евидентирање и управување со животниот циклус на класифицираните информации.

6.1. Класификација и означување

Сите информации мора да бидат класифицирани веднаш по нивното создавање или прием. Класификацијата ја врши создавачот на информацијата или овластено лице.

Сите класифицирани информации мора:

- да бидат јасно означени со соодветното ниво на класификација;
- да содржат TLP-ознака;
- да бидат соодветно означени и во електронска и во физичка форма.

6.2. Прием и евидентирање на класифицирани информации

Сите примени класифицирани информации мора да бидат евидентирани во соодветен регистар, со цел обезбедување следливост и одговорност.

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

Регистарот треба да ги содржи следните податоци:

- датум на прием;
- испраќач;
- ниво на класификација;
- број на примероци;
- определен чувар на информацијата.

Со цел да се обезбеди конзистентна примена, организацијата воспоставува структуриран работен тек што го опфаќа целиот животен циклус на информациите — од нивното создавање до нивното безбедно уништување. Оваа рамка ги дефинира клучните чекори, одговорните улоги и очекуваните активности, со цел обезбедување транспарентност, конзистентност и усогласеност со законските и интерните барања за заштита на класифицираните информации.

Чекор	Активност	Одговорна улога	Опис
1	Создавање или прием на информација	Вработен / создавач на информација	Секоја нова информација се разгледува со цел да се утврди дали содржи чувствителни или класифицирани податоци.
2	Проценка на чувствителност	Создавач + раководител на организациска единица	Се проценува потенцијалното влијание од неовластен пристап, откривање или губење на информацијата.
3	Утврдување на ниво на класификација	Овластено лице / раководител	Се доделува соодветно ниво на класификација (ДРЖАВНА ТАЈНА, СТРОГО ДОВЕРЛИВО, ДОВЕРЛИВО, ИНТЕРНО).
4	Означување	Создавач на информација	Информацијата се означува во електронска и/или хартиена форма.
5	Евидентирање и водење записи	Службеник за безбедност / овластена служба	Документот, примероците и корисниците се евидентираат и се води соодветна документација.

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

6	Складирање и пристап	Сопственик на информација + ИТ оддел	Се применуваат мерки за физичка и техничка заштита, како и контрола на пристап.
7	Користење и обработка	Овластени корисници	Информацијата се користи исклучиво за службени цели и во согласност со принципот „потреба да се знае“.
8	Споделување	Овластено лице / службеник за безбедност	Споделувањето се врши преку безбедни канали и соодветно се евидентира.
9	Прекласификација / декласификација	Создавач / овластено лице	Се вршат периодични прегледи за утврдување на потребата од понатамошна класификација.
10	Архивирање	Архива / овластена служба	Информацијата се чува во согласност со утврдените рокови за чување.
11	Уништување	Овластена комисија / службеник за безбедност	Информацијата се уништува на безбеден начин, при што уништувањето се евидентира.

6.3. Складирање, ракување и контрола на класифицирани информации

Класифицираните информации се складираат, обработуваат и користат исклучиво под соодветни безбедносни услови и строго за службени цели, во согласност со законските барања и утврдените организациски процедури.

Организацијата воспоставува интегриран систем за управување со класифицирани информации кој ги опфаќа следните области:

- **Управување со животниот циклус на информации**

  Се воспоставуваат процедури за управување со целокупниот животен циклус на класифицираните информации, вклучувајќи:

  - создавање и означување на информации;
  - безбедно складирање во електронска и физичка форма;
  - контролирано користење и обработка;
  - контролирано споделување и пренос;

- прекласификација и декласификација, кога е применливо;
- архивирање;
- безбедно отстранување и уништување.

➢ **Контрола на пристап и користење**

Се применуваат мерки за:

- обезбедување контрола на пристап врз основа на принципот „потреба да се знае“;
- спречување на неовластено копирање, откривање или дистрибуција;
- следење и контрола на користењето на информациите.

➢ **Контрола на дигитални канали**

Се применуваат технички мерки за заштита на електронските информации, вклучувајќи:

- енкрипција на чувствителни податоци;
- користење на безбедни комуникациски канали;
- контрола на пристап до информациските системи;
- следење и евидентирање на пристапот и активностите за споделување на информации.

➢ **Одговорности и управување со инциденти**

Јасно се дефинираат улогите и одговорностите за:

- службеникот за безбедност на класифицирани информации;
- раководството;
- вработените и корисниците на информации.

Се воспоставуваат процедури за евидентирање, контрола и навремено пријавување на безбедносни инциденти.

➢ **Обука и подигање на свеста**

Организацијата обезбедува редовни обуки и програми за подигање на свеста кои опфаќаат:

- правилно ракување со класифицирани информации;
- примена на TLP класификацијата;
- усогласеност со безбедносните процедури.

➢ **Контрола и ревизија**

Се воспоставува процес за редовен преглед и ревизија на:

- имплементацијата на безбедносните мерки;
- правилното означување на информациите;
- процесите на споделување и евидентирање.

Овие активности придонесуваат кон институционална зрелост и обезбедуваат континуирана усогласеност со законската рамка и релевантните стандарди.

6.4. Репродукција, превод и изводи

Репродукцијата (копирањето), преводот или изработката на изводи од класифицирани информации е дозволена исклучиво кога постои службена потреба и со претходно одобрение.

При тоа мора да се обезбеди:

- контрола на бројот на изработени примероци;
- евидентирање на овластените корисници;
- задржување на првично утврденото ниво на класификација.

6.5. Дистрибуција на класифицирани информации

Споделувањето на информации се врши строго во обем неопходен за постигнување на утврдената оперативна цел, во согласност со принципот на пропорционалност и минимално неопходно откривање.

Споделувањето на класифицирани информации е дозволено исклучиво:

- во согласност со принципот „потреба да се знае“;
- на лица со соодветно ниво на овластување;
- во согласност со доделената TLP-класификација.

Секое споделување мора да биде контролирано и соодветно евидентирано.

6.6. Пренос на класифицирани информации

Преносот на класифицирани информации мора да се врши исклучиво преку одобрени и безбедни канали.

Електронскиот пренос мора да вклучува:

- енкрипција;
- заштита со лозинка;
- користење на безбедни комуникациски канали.

6.7. Отстранување и уништување

Класифицираните информации мора да бидат безбедно уништени кога повеќе не се потребни или по истекот на утврдените рокови за чување.

Методите на уништување мора да обезбедат спречување на:

- повторна реконструкција на информациите;
- неовластен пристап;

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

- злоупотреба на податоците.

7. Физичка безбедност

Министерството за дигитална трансформација воспоставува физички и технички мерки за заштита со цел спречување на неовластен пристап до класифицирани информации во сите објекти и локации каде што тие се чуваат, обработуваат или користат.

Физичката безбедност има за цел:

- спречување на неовластен пристап;
- одвраќање и откривање на неовластени активности;
- ограничување на пристапот во согласност со принципот „потреба да се знае“.

7.1. Области на примена

Мерките за физичка безбедност се применуваат на:

- објектите и просториите на организацијата;
- канцелариите и работните простори;
- архивите и просториите за складирање;
- серверските простории и просториите за ИКТ;
- сите локации каде што се чуваат или обработуваат класифицирани информации.

7.2. Контрола на физички пристап

Организацијата воспоставува контрола на пристап до просториите во кои се ракува со класифицирани информации. Мерките опфаќаат:

- контролирано влегување и излегување;
- идентификација на вработените и посетителите;
- придружба на посетителите во безбедносно чувствителни простории;
- водење евиденција за пристап до чувствителни простории.

7.3. Безбедносни зони

Просториите во кои се чуваат информации класифицирани како ПОТВРДЕНО или повисоко се определуваат како безбедносни зони.

Зголемените мерки во овие зони вклучуваат:

- построга контрола на пристапот;
- надзор и заштита;
- ограничување на неовластено присуство.

7.4 Технички мерки за заштита

Се применуваат соодветни технички заштитни мерки согласно минималните стандарди утврдени од надлежните органи, кои вклучуваат:

- системи за контрола на пристап;
- алармни системи;
- видео надзор;
- системи за заклучување и заштита на објектите;
- заштита на серверските простории и просториите за ИКТ.

7.5. Пристап според принципот „потреба да се знае“

Физичкиот пристап до објектите и информациите е ограничен на лица со легитимна деловна потреба и со соодветна овластеност, обезбедувајќи дополнителна заштита против неовластен пристап и компромитирање на информациите.

7.6. Пристап до класифицирани информации

Пристапот до класифицирани информации е строго контролиран и се овозможува само на лица и организации кои ги исполнуваат законските критериуми и имаат официјална потреба за пристап. Овој принцип претставува клучна мерка за заштита против неовластено користење, откривање или злоупотреба на класифицираните информации.

7.7. Овластени корисници на класифицирани информации

Овластените корисници може да вклучуваат:

- државни органи и институции;
- правни лица формирани од државата или локалната самоуправа;
- физички и правни лица во Република Северна Македонија со валидно безбедносно одобрение;
- странски државни органи, институции или правни лица со валидно безбедносно одобрение и овластување за пристап издадено од надлежниот орган.

7.8. Безбедносно одобрение

Пристапот до класифицирани информации се овозможува само на лица кои:

- поседуваат соодветно безбедносно одобрение;
- се овластени за пристап до соодветното ниво на класификација;
- се формално одобрени од страна на организацијата.

7.9. Принцип „потреба да се знае“

Дури и кога лице поседува валидно безбедносно одобрение, пристапот до специфични информации се овозможува само доколку е потребно за извршување на службените задачи.

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

Овој принцип обезбедува:

- ограничување на пристапот до минимално неопходниот опсег;
- намалување на ризикот од компромитирање на информациите;
- јасна одговорност за користење на информациите.

7.10. Постапка за одобрување на пристап

Организацијата воспоставува постапки за одобрување, евидентирање и преглед на пристапот до класифицирани информации со цел обезбедување контрола и трагот на користењето на информациите.

7.11. Институционални обврски во однос на безбедносните одобренија

Во согласност со Законот за класифицирани информации, пристапот до класифицирани информации може да им се овозможи само на лица кои поседуваат соодветно безбедносно одобрение и имаат официјална потреба за пристап.

7.12. Барање за безбедносно одобрение

Вработените чија улога и одговорности бараат пристап до класифицирани информации мора да обезбедат соодветно безбедносно одобрение издадено од надлежниот орган.

Безбедносно одобрение е особено потребно за:

- вработени во Секторот за сајбер-безбедност;
- членови на Владинскиот CERT/CSIRT;
- лица кои ракуваат со класифицирани информации;
- лица вклучени во управување со инциденти;
- лица овластени за размена на чувствителни информации со национални и меѓународни партнери.

Нивото на безбедносно одобрение се определува врз основа на работните одговорности и нивото на класификација на информациите со кои се ракува.

7.13. Барање за обука

Лицата со пристап до класифицирани информации мора да ја завршат соодветната обука која опфаќа:

- ракување со класифицирани информации;
- примена на принципот „потреба да се знае“;
- користење на Протоколот на сообраќајните светла (Traffic Light Protocol – TLP);
- постапки за постапување при безбедносни инциденти.

7.14. Институционална обврска за воспоставување заштитни мерки

Државните и локалните органи, правните лица формирани од државата или општините, како и други правни лица, се обврзани да:

- создадат неопходни услови за заштита на класифицираните информации;
- спроведат мерки за намалување на негативните последици во случај на откривање на класифицирани информации;
- воспостават ефективен и координиран систем за управување со класифицирани информации;
- именуваат службено лице за безбедност одговорно за координација и надзор над спроведувањето на заштитните мерки.

Целта е да се обезбеди дека сите активности кои вклучуваат класифицирани информации се изведуваат безбедно и во согласност со законските обврски.

7.15. Службено лице за безбедност на класифицирани информации

Министерството за дигитална трансформација именува Службено лице за безбедност на класифицирани информации во согласност со Законот за класифицирани информации и релевантната подзаконска регулатива. Службеното лице за безбедност претставува централна точка за координација и надзор на системот за заштита на класифицирани информации во институцијата.

7.16. Надлежности на Службеното лице за безбедност

Службеното лице за безбедност е одговорно за:

- координирање на спроведувањето на административните, физичките и техничките мерки за заштита;
- евидентирање и известување за инциденти поврзани со класифицирани информации;
- следење на примената на принципот „потреба да се знае“ при овозможување пристап;
- надзор на правилното ракување, чување и размена на класифицирани информации;
- координација на активности за обука и подигање на свеста;
- подготовка и следење на годишни планови и активности поврзани со заштитата на класифицираните информации;
- соработка со надлежните државни органи во областа на заштита на класифицираните информации.

8. Ракување со информации добиени од FIRST и други CSIRT тимови

Министерството за дигитална трансформација, преку својот CSIRT тим, учествува во национална и меѓународна размена на информации поврзани со сајбер-безбедносни инциденти, закани, ранливости и мерки за ублажување.

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

Информациите добиени од заедницата FIRST, од други национални и меѓународни CSIRT/CERT тимови, како и од доверливи партнери и соработници, се третираат како чувствителни оперативни информации и се ракува со нив со зголемена доверливост и заштитни мерки, согласно оваа политика, примената на Протоколот на сообраќајните светла (TLP) и принципот „потреба да се знае“.

8.1. Задржување на ознаки и ограничувања

Секоја информација добиена од FIRST или друг CSIRT тим:

- го задржува оригиналното TLP означување;
- не смее да се прекласифицира без согласност од изворот;
- не смее да се споделува надвор од опсегот дозволен со доделеното TLP означување.

Доколку информацијата содржи дополнителни ограничувања или услови за користење и споделување, тие ограничувања имаат предност и мора строго да се почитуваат.

8.2. Ракување со информации без TLP означување

Доколку информацијата е примена без јасно дефинирана TLP класификација, CSIRT тимот:

- ја оценува чувствителноста на информацијата;
- оделува соодветна TLP класификација пред понатамошна употреба или споделување;
- ја третира информацијата како минимум TLP AMBER+STRICT додека не се утврди нејзиниот статус.

8.3. Внатрешна употреба и ограничување на пристапот

Информациите добиени од FIRST и други CSIRT тимови може да се споделуваат исклучиво за внатрешна употреба:

- со персонал кој има службена потреба за пристап;
- во обем неопходен за извршување на доделените задачи;
- во согласност со принципот „потреба да се знае“.

Пристапот до ваквите информации треба да биде ограничен на минималниот број овластен персонал што е неопходен.

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

8.4. Ограничувања за понатамошно споделување

Информациите добиени од FIRST и други CSIRT тимови не смеат да се споделуваат со:

- јавноста;
- медиумите;
- неовластени лица или организации, освен ако:изворот има дадено изречна согласност; или
- TLP класификацијата дозволува такво споделување.

При понатамошно споделување на информациите, задолжително мора да се задржат:

- оригиналната TLP класификација;
- изворот на информациите;
- сите ограничувања утврдени од изворот.

8.5. Водење евиденција и следливост

CSIRT треба да води евиденција за:

- приемот на информации од FIRST и други CSIRT тимови;
- нивната обработка и користење;
- секое понатамошно споделување, кога е дозволено.

Овие евиденции треба да се одржуваат со цел да се обезбедат доверливост, отчетност и следливост во процесот на размена на информации.

9.Ракување со класифицирани и чувствителни информации на преносливи уреди и надвор од службени простории

Со цел да се намали ризикот од неовластен пристап, губење или компромитирање на информации, Министерството воспоставува правила за користење на преносливи уреди и обработка на информации надвор од службените простории.

Овие правила се применуваат на:

- службени лаптопи;
- мобилни телефони;
- таблет уреди;
- работа на далечина и работа од дома;
- пристап до службени информации преку надворешни мрежи.

9.1. Основни принципи

Класифицираните и чувствителни информации може да се обработуваат надвор од службените простории само кога тоа е неопходно за извршување на службените должности и во согласност со соодветни технички и организациски мерки за заштита.

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

Користењето на лични уреди за обработка на класифицирани информации е строго забрането.

9.2. Складирање на информации на преносливи уреди

За службени лаптопи и мобилни уреди:
Информации означени како TLP RED и TLP AMBER+STRICT:

- не смеат трајно да се складираат локално без претходно одобрување;
- мора да бидат заштитени со енкрипција;
- мора да се складираат исклучиво во одобрени информациски системи;
- мора да бидат обезбедени со механизми за автентикација и контрола на пристап.

Информации означени како TLP GREEN:

- Може да се обработуваат на службени уреди со примена на стандардните мерки за безбедност.

Информации означени како TLP CLEAR:

- Може да се обработуваат без дополнителни ограничувања.

Дистанциска работа и користење на надворешни мрежи

При пристап до службени системи од надворешни мрежи, треба да се применуваат следните мерки:

- Користење на сигурни VPN врски;
- Мултифакторска автентикација;
- Користење исклучиво на службени уреди;
- Избегнување на јавни или несигурни безжични мрежи.

Обработката на класифицирани информации на јавни места (аеродроми, хотели, јавни простори) треба да се избегнува, освен ако е строго неопходна, и во тој случај да се извршува со зголемена претпазливост.

Комуникација преку мобилни и несигурни канали

Информации означени како TLP RED и TLP AMBER+STRICT не смее да:

- Се дискутираат преку лични мобилни телефони;
- Се пренесуваат преку несигурни комуникациски апликации;
- Се споделуваат преку лични е-пошта сметки;
- Се обработуваат преку неслужбени канали за комуникација.

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

Осетливите информации мора да се комуницираат исклучиво преку:

- Одобрени службени канали за комуникација;
- Сигурни платформи за комуникација;
- Службена е-пошта со применети мерки за безбедност.

Заштита во случај на губење или кражба на уред

Во случај на губење или кражба на службен уред, корисникот веднаш треба да го извести одговорниот сектор за ИКТ и службеникот за безбедност.

Министерството спроведува мерки за:

- Далечинско заклучување или бришење на податоците;
- Спречување на неовластен пристап;
- Запишување и анализа на инцидентот.

10. Објавување на информации и јавна комуникација од CSIRT

За да се обезбедат транспарентност, доверба и координиран одговор на кибер инциденти, Министерството воспоставува правила за објавување на информации од тимот CSIRT до јавноста, засегнатите страни и партнерските организации.

Објавувањето на информации мора да биде во согласност со:

- Применливиот правен рамки;
- Принципот „потреба за знаење“ (need-to-know);
- Примената на TLP (Traffic Light Protocol);
- Обврските за доверливост кон пријавувачите и партнерите.

Овластување за јавни изјави

Јавни изјави, соопштенија за медиуми и информации поврзани со инциденти во сајбер безбедноста можат да се издаваат исклучиво:

- Од овластено лице;
- Преку службените канали за комуникација на институцијата.

Членовите на CSIRT тимот не смеат самоволно да даваат изјави за медиуми или јавност без претходно одобрување од раководството.

Информации дозволени за јавно објавување

Информации може да се објавуваат јавно ако:

- Се означени како TLP CLEAR
- Се агрегирани и анонимизирани;
- Претставуваат предупредувања, препораки или упатства за безбедност;
- Имаат цел да ја подигнат јавната свесност;
- Не овозможуваат идентификација на засегнатите организации или поединци.

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

Информации забранети за јавно објавување

Следниве информации не смее да се објавуваат јавно:

- Детали за тековни или активни инциденти;
- Технички информации кои би можеле да се злоупотребат;
- Информации кои би можеле да ги идентификуваат жртвите;
- Податоци добиени од други CSIRT тимови без нивна согласност;
- Информации означени како TLP RED или TLP AMBER+STRICT.

10.1 Комуникација со засегнатите организации (жртви на инциденти)

CSIRT обезбедува доверлива и контролирана комуникација со организации и поединци засегнати од инциденти.
При комуникација со засегнатите страни:

- Се споделуваат само информации кои се неопходни за ублажување и решавање на инцидентот;
- Се почитува доверливоста на пријавувачите;
- Информациите не се споделуваат со трети страни без согласност, освен ако тоа е законски задолжително.

Засегнатите страни можат да очекуваат дека дадените информации ќе се користат исклучиво за управување и координација на инцидентот.

10.2. Споделување информации со други CSIRT тимови

CSIRT може да споделува информации со други национални и меѓународни тимови кога е потребно за:

- Превенција или ублажување на инциденти;
- Координација на одговор на закани;
- Заштита на критичната инфраструктура.

Споделувањето информации мора секогаш да биде во согласност со:

- Ограничувањата на TLP;
- Договорите и обврските за доверливост;
- Законските барања.

10.3. Јавна достапност на ограничувањата

Министерството обезбедува јавна достапност на основните принципи за доверливост и објавување информации, за засегнатите страни и партнерите да имаат јасни очекувања за ракувањето со доставените информации.

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

11.Доверливост на информациите доставени од пријавувачи на инциденти

CSIRT обезбедува доверливо ракување со сите информации доставени од организации, институции и поединци при пријавување на сајбер инциденти, ранливости и закани.
Целта е да се изгради доверба и да се поттикне навремено пријавување на инциденти.

11.1. Принцип на доверливост на пријавувачот

Информациите добиени при пријавување на инциденти се сметаат за доверливи и се користат исклучиво за:

- Анализа и обработка на инцидентот;
- Координација на напорите за одговор;
- Превенција на понатамошна штета;
- Зголемување на националната сајбер безбедност.

Идентитетот на пријавувачот нема да се открие без претходна согласност, освен кога тоа е законски задолжително.

11.2. Ограничен пристап до доставените информации

Пристапот до информациите доставени од пријавувачите е ограничен на:

- Членови на CSIRT тимот;
- Овластено лице во институцијата кога е потребно за ракување со инциденти;
- Надлежни органи кога е законски задолжително.

Сите лица со пристап до овие информации се обврзани да ја одржуваат нивната доверливост.

11.3. Споделување информации со трети страни

Информациите доставени од пријавувачите може да се споделуваат со трети страни само кога:

- Е потребно за решавање на инцидентот;
- Е законски задолжително;
- Се добиена претходна согласност од пријавувачот;
- Информациите се анонимизирани и не овозможуваат идентификација.

11.4. Анонимизација и агрегирање на податоци

CSIRT може да користи агрегирани и анонимизирани податоци за:

- Статистичка анализа;
- Извештајување;
- Иницијативи за јавна свесност;

- Подобрување на заштитните мерки.

Таквите податоци не смеат да овозможат идентификација на пријавувачот или на засегнатата организација.

11.5. Очекувања на пријавувачот

Организациите и поединците кои пријавуваат инциденти можат да очекуваат дека:

- Нивните информации ќе се третираат како доверливи;
- Информациите нема да се објавуваат јавно без оправдување;
- CSIRT ќе постапува во согласност со принципите на доверба, професионализам и законитост.

12. Јавно достапни ограничувања за објавување информации

За да се обезбеди транспарентност и јасни очекувања кај засегнатите страни, Министерството ги објавува основните принципи и ограничувања поврзани со објавувањето информации од CSIRT.
Овие ограничувања се јавно достапни со цел да се изгради доверба и да се поттикне соработка при пријавувањето и ракувањето со сајбер инциденти.

12.1. Информации што CSIRT може да ги објави

CSIRT може јавно да објави информации кои:

- Се означени како TLP CLEAR;
- Се агрегирани и анонимизирани;
- Се однесуваат на трендови, статистики и општи закани;
- Се објавуваат предупредувања и препораки за безбедност;
- Не овозможуваат идентификација на засегнатите организации или поединци;
- Не го загрозуваат тековното ракување со инциденти.

12.2. Информации што CSIRT не ги објавува

CSIRT не објавува јавно:

- Информации означени како TLP RED или TLP AMBER+STRICT;
- Информации за тековни или нерешени инциденти;
- Технички детали кои би можеле да се злоупотребат;
- Идентитет на засегнати организации или поединци;
- Информации добиени од други организации или CSIRT тимови без нивна согласност;
- Информации подложни на законски ограничувања или класификација.

12.3. Ограничувања при објавување

Објавувањето на информации може да биде ограничено кога:

- Постои ризик за националната безбедност;
- Постои ризик од дополнителна штета или злоупотреба;
- Информацијата е дел од тековна истрага;
- Се применуваат договорни или законски обврски за доверливост.

12.4. Цел на ограничувањата

Овие ограничувања имаат за цел:

- Заштита на засегнатите страни;
- Превенција од дополнителни сајбер закани;
- Одржување доверба со партнерите;
- Обезбедување усогласеност со законските и меѓународните обврски.