Република Северна Македонија

Министерство за дигитална трансформација

ПРАВИЛНИК ЗА ЕТИЧКО ОДНЕСУВАЊЕ НА MKD-GOV-CSIRT

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

Овие правила за етичко однесување се донесуваат во согласност со Законот за безбедност на мрежни и информациски системи и во насока на усогласување со барањата на Директивата (ЕУ) 2022/2555 (NIS2). Истите претставуваат составен дел од институционалната рамка за функционирање на Владиниот тим за одговор на компјутерски безбедносни инциденти (MKD-GOV-CSIRT), со цел обезбедување доверливост, професионалност, интегритет и транспарентност во постапувањето.

1. Цел и опфат

Овој документ ги дефинира принципите и стандардите за етичко однесување на MKD-GOV-CSIRT, со цел:

- Усогласување со SIM3 моделот за зрелост;
- Правилата се усогласени со Code of Ethics на FIRST (Forum of Incident Response and Security Teams) и служат како интерен документ за поддршка на членството и активното учество на MKD-GOV-CSIRT во FIRST заедницата;
- MKD-GOV-CSIRT постапува во добра намера и во интерес на националната и глобалната сајбер безбедност, во согласност со принципите на FIRST заедницата

Документот важи за сите вработени, соработници и ангажирани експерти кои работат под надлежност на MKD-GOV-CSIRT. Оваа рамка вклучува принципи формулирани како изјави за одговорност, врз основа на разбирањето дека јавното добро е секогаш примарна грижа. Секој принцип е дополнет со упатства, кои даваат објаснувања за да им помогнат на компјутерските професионалци во разбирањето и примената на принципот.

2. Основи етички принципи (FIRST Code of Ethics)

MKD-GOV-CSIRT ги прифаќа и применува следните должности кои се во согласност со основните етички принципи на FIRST (Code of Ethics) :

2.1 Должност за доверба и соработка

MKD-GOV-CSIRT активно соработува со други CSIRT тимови и институции, градејќи односи базирани на доверба. Довербата е основа на многу односи меѓу тимовите и често е потребна пред да може да се случи значајна размена на информации. FIRST заедницата е изградена врз основа на оваа доверба и може да продолжи да функционира на овој начин само ако постои разумно ниво на доверба меѓу тимовите.
Доверливоста значи дека членовите на тимот треба само:

1) да преземат обврски што можат да ги исполнат;
2) да се однесуваат предвидливо кон другите тимови (на пр., да ги почитуваат TLP стандардите);
3) да го одржуваат доверливиот однос што го имаат со другите тимови. Доверливиот однос треба првично да се претпостави и да биде транзиторен, т.е. Доверба при прва употреба (TOFU) и да овозможи доверба за тимовите на кои им веруваат другите тимови.

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

2.2 Должност за координирано откривање на ранливост

Членовите на тимот кои ќе дознаат за ранливост треба преку соработка со засегнатите страни да работат на санирање на безбедносната ранливост и минимизирање на штетата поврзана со откривањето. Засегнатите страни вклучуваат, но не се ограничени на: известувачот за ранливост, засегнатите добавувачи, координаторите, бранителите и клиентите, партнерите и корисниците. Членовите на тимот треба да се координираат со соодветните засегнати страни за да се договорат за јасни временски рокови и очекувања за објавување на информации, обезбедувајќи доволно детали за да им овозможат на корисниците да го проценат својот ризик и да преземат акциони одбранбени мерки.

2.3 Обврска за доверливост

Членовите на тимот имаат должност да одржуваат доверливост каде што е соодветно. Барањата за чување на одредени доверливи информации може да бидат експлицитни, на пример, со Traffic Light Protocol (TLP). Членовите на тимот треба да ги почитуваат таквите барања секогаш кога е можно. Доколку не е можно да се чуваат доверливи, на пример, поради конфликти со барањата на локалните закони, договори или должност за информирање, членот на тимот треба веднаш да го извести сопственикот на информациите за овој конфликт.
Некои должности за доверливост се засноваат на закони, прописи или обичаи. Доколку, за време на одговор на инцидент, некои страни се обврзани или очекуваат доверливост врз основа на такви размислувања, тие треба да се потрудат овие очекувања да ги направат експлицитни однапред.

2.4 Обврска за потврда

Тимовите добиваат информации од многу различни извори: истражувачи, клиенти, други тимови, владини субјекти итн. Членовите на тимот треба навремено да одговорат на барањата, дури и ако тоа е само за да потврдат дека барањето е примено. Кога е можно, членовите на тимот треба да постават очекувања за следното ажурирање.

2.5 Должност за овластување

Членовите на тимот имаат легитимна потреба и право да ги разберат своите области на одговорност, дејствувајќи само врз системи до кои имаат овластување за пристап. Членовите на тимот треба да бидат свесни за тоа како нивните дејствија можат да влијаат врз нивните конституенти и да се осигураат дека не предизвикуваат дополнителна штета додека ги извршуваат своите должности. Каде што е можно, конституентите треба да бидат консултирани пред да се направат промени во нивните системи.

2.6 Должност за информирање

Членовите на тимот треба да сметаат дека е нивна должност да ги информираат своите конституенти за тековните безбедносни закани и ризици. Кога членовите на тимот имаат информации што можат негативно да влијаат или да ја подобрат безбедноста и сигурноста, тие

имаат должност да ги информираат релевантните страни или други лица кои можат да помогнат, со соодветен напор, притоа земајќи ги предвид доверливоста, законите и прописите за приватност и други обврски.

2.7 Почитување на приватноста и човековите права

Членовите на тимот треба да бидат свесни дека нивните постапки можат да влијаат врз човековите права на другите преку споделување информации, можна пристрасност во нивните постапки или повреда на правата на сопственост. Членовите на тимот имаат пристап до широк спектар на лични, чувствителни и доверливи информации во текот на справувањето со инциденти. Овие информации треба да се обработуваат на начин што ги почитува човековите права.
За време на справувањето со инциденти, лицата кои реагираат не треба да дејствуваат пристрасно и треба да сторат сè што можат за да ја елиминираат пристрасноста од нивните процеси и донесување одлуки.

За целите на овој принцип, поимот „сопственост“ (Декларација на ОН за човекови права: Член 17) вклучува нематеријални добра како што е интелектуалната сопственост, како и идеи и концепти воопшто, без оглед на тоа дали се законски заштитени (на пр., патентирани).

2.8 Должност кон здравјето на тимот

Тимовите имаат одговорност да продолжат да ги обезбедуваат услугите што им ги ветиле на своите конституенти. Оваа одговорност го вклучува физичкото и емоционалното здравје на тимот. За да се почитуваат членовите што го сочинуваат тимот како поединци и да се овозможи долгорочна одржливост на соодветно ниво на услуга, тимот треба да се стреми да одржува здрава, безбедна и позитивна работна средина што го поддржува физичкото и емоционалното здравје на сите негови членови.

2.9 Должност за развој на капацитети на тимот

Управувањето со инциденти е тема во развој што членовите на тимот треба постојано да ја изучуваат. Тимот треба да им обезбеди ресурси на своите членови за да можат да изучуваат, применуваат и унапредуваат технолошко и научно знаење во рамките на нивната област и одговорност. Обуката или образовните кредити за CPE/CEU може да придонесат, но само вежбите за усогласеност не се доволни за да се исполни оваа должност. Тимот треба да одржува доволна технолошка инфраструктура за да ги овозможи своите услуги, вклучително и соодветни мерки за заштита на таа инфраструктура од мешање од надворешни страни.

2.10 Должност за одговорно собирање податоци

Собирањето податоци е неопходно за одговор на инцидент, но треба да се воспостави рамнотежа помеѓу целта на одговор на инцидент и почитувањето на засегнатите страни. За време на истрагата, количината на информации потребни за собирање може да се промени. Додека се работи на инцидентот, членовите на тимот треба да го прилагодат она што го собираат како што се менува потребата. Податоците што не се директно релевантни за инцидентот и неговото санирање треба да бидат исклучени од известувањето.

Собраните и извлечените податоци мора да се обработуваат во согласност со важечките закони и почитувањето на приватноста на корисниците. Треба да се побара дозвола пред собирање и обработка на податоци под контрола на сопственикот на податоците. Треба да се

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

почитуваат важечките закони и прописи за ракување со податоци. Податоците што можат да им помогнат на другите тимови за одговор во нивните напори поврзани со други инциденти треба да им бидат достапни, по можност во редактирана форма. Информациите што се доверливи и заштитени треба да бидат достапни само со соодветна заштита.
Пред да се споделат податоци со трети страни за ублажување, ризиците треба да се споредат со придобивките. Податоците треба да се споделуваат само ако придобивката јасно ги надминува ризиците. Чувствителните податоци треба да се чуваат на начин што лесно ќе можат да се уништат откако ќе се реши инцидентот. Собраните податоци треба безбедно да се уништат во согласност со политиките за задржување на податоци.

2.11 Должност за почитување на правни и институционални надлежности

Членовите на тимот треба да ги признаваат и почитуваат правните и институционалните надлежности, законските права, правилата и овластувањата на страните вклучени во активностите поврзани со одговор на инциденти.

Законите, прописите и другите правни прашања, како што се оние поврзани со заштитата на приватноста или известувањата за повреда на податоци, може да се разликуваат помеѓу различни правни системи, држави или сектори. Надлежностите може да бидат утврдени од физичките локации на вклучените страни, како што се нивните земји или живеалишта, како и од други фактори што се однесуваат на тие страни. Дури и во рамките на една земја, законите и прописите може да се разликуваат помеѓу политичките региони (на пр., помеѓу поединечни држави во САД) или помеѓу различни бизниси, индустрии или сектори во таа нација (на пр., здравствена заштита, финансиски услуги и владини објекти). Националните CSIRT може да имаат назначени одговорности и/или овластувања за активности што вклучуваат составни делови во рамките на нивната сопствена јурисдикција, а тие исто така можат да соработуваат со или да „предаваат“ информации и активности на други субјекти кои имаат овластувања за јурисдикции што ги преминуваат границите.

Членовите на тимот треба да бидат свесни за клучните прашања што влијаат на вклучените јурисдикции, вклучувајќи, но не ограничувајќи се на прописите за приватност или барањата за известување за повреда на податоци. Бидејќи законите и прописите за сајбер безбедност и приватност еволуираат и продолжуваат да се ажурираат низ целиот свет, препорачливо е да се консултирате со информиран правен советник за насоки секогаш кога прашањата вклучуваат повеќе правни или институционални надлежности.

2.12 Должност за расудување базирано на докази и факти

Тимовите треба да работат врз основа на проверливи факти. При споделување информации, како што се индикатори за компромис (IOC) или описи на инциденти, членовите на тимот треба транспарентно да обезбедат докази и обем. Доколку тоа не е можно, причините за не споделување на овие докази и обем треба да бидат наведени со информациите.

Членовите на тимот треба да се воздржат од ширење или споделување гласини. Секоја хипотеза треба јасно да биде идентификувана како таква.

Транспарентните процеси на докази и расудување се важни дури и во случај на автоматско споделување, на пр., за време на автоматско споделување на големи количини на информации. Во овој случај, описот
на процесот на собирање на податоци треба да се соопшти на разбирливо ниво на детали.

3. Справување со дилеми

Членовите на тимот често може да се најдат во позиција каде што ниту една акција не ги задоволува сите етички принципи. Во таква ситуација, мора да се направи избор за тоа кои принципи да се приоретизираат. Во оваа ситуација, лицата кои се занимаваат со инциденти се охрабруваат да размислат за тоа кои засегнати страни може да бидат засегнати од нивните постапки и како, по можност во дискусија со колега. Како по правило, треба да се избере решението што го минимизира кршењето на оваа етичка рамка. Понекогаш, ова може да не биде можно, на пр. поради надворешни притисоци. Во таква ситуација, се препорачува да се продолжи, имајќи ја предвид етичката дилема.

4.Усогласеност со SIM3 моделот

MKD-GOV-CSIRT:

- Го применува овој правилник заедно со P11 – Интерен документ за безбедно управување со информации и другите поврзани политики за заштита и обработка на информации**;**
- Одржува формални процедури за управување со инциденти во согласност со SIM3 домените: Организација, Луѓе, Процеси и Алатки;
- Обезбедува јасни улоги и одговорности;
- Применува контроли за доверливост, интегритет и достапност;
- Документира активности за целите на ревизија и унапредување.

5. Практични правила за однесување

- Забрането е неовластено откривање на информации.
- Забрането е користење на доверливи податоци за лична корист.
- Секој конфликт на интерес мора веднаш да се пријави.
- Сите активности мора да бидат документирани и ревидирани

6.Обука и свесност

MKD-GOV-CSIRT обезбедува редовни обуки за:

- FIRST Code of Ethics;
- SIM3 контролите;
- TLP правилна примена;
- Заштита на лични податоци и класифицирани информации.

7.Непочитување и санкции

Прекршувањето на овие правила може да повлече дисциплинска, прекршочна или друга одговорност, во согласност со важечкото национално законодавство.

8.Преглед и подобрување

Документот се ревидира најмалку еднаш годишно или по промени во FIRST стандардите, SIM3 моделот или законодавството.

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