УПАТСТВО ЗА ПРИЈАВА НА ИНЦИДЕНТИ ОД КОНСТИТУЕНТИ

I. ОПШТИ ОДРЕДБИ

Член 1

Со ова упатство се уредуваат начинот на пријава на сајбер безбедносни инциденти од страна на конституентите на MKD-GOV-CSIRT, содржината на пријавата, роковите за известување, како и постапувањето по пријавени инциденти. Со упатството се уредуваат и надлежностите, улогата и услугите што ги обезбедува тимот за одговор на компјутерски инциденти MKD-GOV-CSIRT.

Член 2

Конституенти на MKD-GOV-CSIRT, се: Владата на Република Северна Македонија, министерствата, самостојните органи на државната управа, органите на државната управа во состав на министерствата, управните организации, општините, општините во градот Скопје и градот Скопје. Конституентите се должни да постапуваат согласно одредбите од овој правилник при пријава и управување со сајбер безбедносни инциденти.

Член 3

Целта на ова упатство е да им помогне на конституенти да го пријават сајбер безбедносниот инцидент до MKD-GOV-CSIRT во бараната временска рамка.

II. ДЕФИНИЦИИ

Член 4

Безбедност на мрежни и информациски системи е способност на мрежните и информациските системи, да се спротивстават, со одредено ниво на доверба, на секое дејство кое ја загрозува достапноста, автентичноста, интегритетот или доверливоста на складираните, пренесените или обработените податоци или на поврзаните услуги што ги нудат или се достапни преку тие мрежни и информациски системи.

Член 5

Значајна сајбер закана е сајбер закана за која врз основа на нејзините технички карактеристики, може да се претпостави дека може да има сериозно влијание врз мрежните и информациските системи на некој субјект или на корисниците на услугите на тој субјект преку предизвикување значителна материјална или нематеријална штета.

Член 6

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

Значаен сајбер безбедносен инцидент е сајбер безбедносен инцидент кој предизвикал или може да предизвика сериозни нарушувања во функционирањето на услугите или да предизвика финансиски загуби за соодветниот клучен, односно важен субјект, влијаел или може да влијае врз други физички или правни лица со предизвикување значителна материјална или нематеријална штета.

Член 7

Инцидент е настан кој ги загрозува достапноста, автентичноста, интегритетот или доверливоста на зачуваните, пренесените или обработените податоци или на услугите понудени од или достапни преку мрежните и информациските системи.

Член 8

Офицер за сајбер безбедност е лице кое задолжително се ангажира кај суштинските субјекти, кое има соодветни посебни работни компетенции, е одговорно за спроведување на мерките за сајбер безбедност утврдени со Законот за безбедност на мрежни и информациски системи („Службен весник на Република Северна Македонија“ бр. 135 од 4.7.2025), е во директна
комуникација и соработува со надлежниот орган и надлежниот тим за одговор на компјутерски инциденти за доследна имплементација на одредбите од истиот закон.

Член 9

Сајбер безбедност е систем на активности и мерки потребни за заштита на мрежните и информациските системи, корисниците на таквите системи и другите лица погодени од закани преку компјутерски мрежи.

Член 10

Сајбер закана е секоја потенцијална околност, настан или активност што може да оштети, наруши или на друг начин негативно да влијае врз мрежните и информациските системи, корисниците на таквите системи и други лица.

Член 11

Тим за одговор на компјутерски инциденти (CSIRT) е тело надлежно за справување со инциденти, согласно пропишана процедура.

Член 12

Суштински субјекти од аспект на безбедност на мрежни и информациски системи се големите субјекти кои припаѓаат на областите енергетика, транспорт, банкарство, финансиски пазар, здравство, дигитална инфраструктура, управување со ИКТ-услуги, снабдување на вода за пиење и дистрибуција, отпадни води, поштенски и курирски услуги, управување со отпад, изработка, производство и дистрибуција на хемикалии, производство, преработка и дистрибуција на храна, производство, даватели на

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

дигитални услуги и истражувања, даватели на квалификувани доверливи услуги, регистар на имиња на врвните домени, (доменот mk и доменот мкд) или давател на ДНС услуги, независно од нивната големина, оператори, односно даватели на јавни електронски комуникациски мрежи и/или јавно достапни електронски комуникациски услуги кои се сметаат за средни и големи субјекти, институциите на јавниот сектор, Собранието, самостојните државни органи и регулаторни тела основани од и одговорни пред Собранието, Владата, министерствата, самостојните органи на државната управа, органите на државната управа, органите на државната управа во состав на министерствата, управните организации, судовите и општините, општините во градот Скопје и градот Скопје, субјектите кои независно од нивната големина припаѓаат на групата субјекти, даватели на доверливи услуги и субјект кој го води Единствениот регистар на врвни домени (доменот mk и доменот мкд), субјектите кои се утврдени како сопственици/оператори на критична инфраструктура, субјекти кои согласно националното законодавство се утврдени како суштински субјекти, други субјект, кои согласно закон или врз основа на направена проценка на ризик се утврдени како суштински субјекти.

Член 13

Важни субјекти, од аспект на безбедност на мрежни и информациски системи се сите субјекти од деталната листа на областите со висока критичност од деталната листа на областите со висока критичност, од деталната листа на области и видови на субјекти од областите со висока критичност кои не спаѓаат во групата на суштинските субјекти и други субјекти, кои согласно закон или врз основа на направена проценка на ризик се утврдени како важни субјекти.

III. НАДЛЕЖНОСТИ И УСЛУГИ НА MKD-GOV-CSIRT

Член 14

MKD-GOV-CSIRT е надлежен за управување и одговор на сите видови компјутерски безбедносни инциденти кои настануваат или можат да настанат во мрежите, информациските системи и услугите на конституентите. Тимот врши следење на безбедносни закани, анализа на инциденти, координација на активностите за одговор и обезбедување стручна поддршка.

Член 15

MKD-GOV-CSIRT обезбедува поддршка на конституентите преку реактивни и проактивни услуги од областа на сајбер безбедноста. Тимот врши континуирано следење и детекција на безбедносни настани, нивна анализа и координација на активностите за управување со инциденти. Во рамки на управувањето со безбедносни инциденти, MKD-GOV-CSIRT врши прием на пријави за инциденти, анализа и координација на активности за нивно решавање, во соработка со засегнатите конституенти.

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

Член 16

MKD-GOV-CSIRT ги координира активностите за управување со инциденти согласно важечката законска регулатива и соработува со националниот тим MKD-CIRT за размена на информации и усогласување на активностите при инциденти со голем опфат.

IV. ПРИЈАВА И ОДГОВОР НА ИНЦИДЕНТИ

Член 17

Конституентите се должни веднаш, а најдоцна во рок од три (3) часа од моментот на дознавање за настанување на инцидентот и/или сајбер заканата, да го известат MKD-GOV-CSIRT за секој значаен сајбер безбедносен инцидент и/или значајна сајбер закана што има влијание врз обезбедувањето на нивните услуги и да ги достават сите информации, со кои ќе овозможат да го утврди прекуграничното влијание на инцидентот.

Навремено пријавување е од суштинско значење за ефикасно управување со инцидентите и намалување на нивното влијание.

Член 18

Конституентите се должни, веднаш, а најдоцна наредниот работен ден од моментот на дознавањето за значајната сајбер закана да ги известат корисниците на нивните услуги на кои може да влијае значајна сајбер закана, за сите мерки или правни средства кои тие можат да ги преземат како одговор на заканата, а доколку е потребно и за самата сериозна сајбер закана.

Член 19

Конституентите се должни во рок од 24 часа од дознавањето за значајниот сајбер безбедносен инцидент до MKD-GOV-CSIRT да достават рано предупредување во коешто доколку е соодветно, ќе се наведе дали постои сомневање дека значајниот инцидент е предизвикан од незаконско или злонамерно дејствување или може да има прекугранично влијание.

Член 20

Конституентите се должни во рок од 72 часа од дознавањето за значајниот сајбер безбедносен инцидент до MKD-GOV-CSIRT да достават известување за инцидентот во коешто:

- ќе ја наведе почетната процена на значителниот инцидент,
- неговата сериозност и влијание,
- показателите за загрозеност, доколку се достапни.

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

Член 21

Во рок од еден месец по доставувањето на известувањето за значајниот сајбер безбедносен инцидент, конституентите се должни до MKD-GOV-CSIRT да достават завршно известување што го вклучува следново:

- детален опис на инцидентот, вклучувајќи ја неговата сериозност и влијание;
- типот на закана или главната причина што најверојатно го предизвикала инцидентот;
- мерките за ублажување што се применили и се применуваат и
- прекуграничното влијание на инцидентот, доколку е соодветно.

Член 22

Во случај кога значајниот сајбер безбедносен инцидент е во тек во моментот на поднесувањето на завршното известување до MKD-GOV-CSIRT, конституентите да достават извештај за напредокот во тој момент, како и завршен извештај во рок од еден месец од решавањето на инцидентот.

Член 23

MKD-GOV-CSIRT е должен во рок од 24 часа од приемот на раното предупредување на конституентот да му достави одговор, вклучувајќи ги првичните повратни информации за значајниот сајбер безбедносен инцидент, а на барање на конституентот, да му даде насоки или оперативни совети за спроведување на можни мерки за ублажување, како и дополнителна техничка поддршка.

Член 24

Доколку MKD-GOV-CSIRT не е прв примател на известувањето, насоките или оперативните совети ги обезбедува надлежниот орган во соработка MKD-GOV-CSIRT.

Член 25

MKD-GOV-CSIRT обезбедува дополнителна техничка поддршка доколку конституентот тоа го побара.

Член 26

Доколку постои сомневање дека со значајниот сајбер безбедносен инцидент е сторено кривично дело, MKD-GOV-CSIRT ќе даде насока истиот да се пријави кај надлежните органи.

Член 27

Доколку за спречување или за решавање на значајниот сајбер безбедносен инцидент што е во тек е потребно да се извести јавноста или доколку откривањето на значителниот инцидент е во интерес на јавноста од некоја друга причина, Министерството за

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

дигитална трансформација може, по извршена консултација со засегнатиот суштинскиот, односно важниот субјект, да ја извести јавноста за значајниот сајбер безбедносен инцидент или да побара од соодветниот субјект да го направи тоа.

Член 28

Секој личен податок во извештаите за значаен сајбер безбедносен инцидент треба да биде ограничен на она што е строго неопходно за опис и решавање на инцидентот.

Член 29

Информацијата се класифицира согласно Политиката за откривање на информации (Traffic Light Protocol) TLP – Clear, Green, Amber, Amber Strict, Red, додека нивото на заштита на доставената информација се определува како: Јавно, Доверливо или Строго доверливо.

Член 30

Пријавата може да се достави преку:

- порталот на Министерството од член 15 став (5) од Законот (основен канал, задолжителен кога е достапен); официјален Образец за пријава на инциденти,
- електронска пошта (електронски потпишана и шифрирана),
- телефонска комуникација во итни случаи.

Член 31

По приемот на пријавата, MKD-GOV-CSIRT доставува потврда до конституентот за регистрација на пријавата, вклучително и број на пријава на инцидент за понатамошна комуникација.

Член 32

По приемот на пријавата од конституент, MKD-GOV-CSIRT започнува со управување со инцидентот согласно своите законски надлежности. Тимот врши идентификација, анализа, координација на одговор и, по потреба, обезбедување техничка поддршка кон конституентот, со цел ефективно управување со сајбер безбедносните закани и инциденти, во согласност со Законот за безбедност на мрежите и информациските системи.

V. ДОБРОВОЛНИ ИЗВЕСТУВАЊА

Член 33

Конституентите може, на доброволна основа, до MKD-GOV-CSIRT да достават известувања за сајбер безбедносни инциденти, сајбер закани и избегнати инциденти (near-misses) кои не се значителни, согласно член 38 од Законот. Субјекти кои не се во опфатот на ова упатство може, исто така, да достават доброволни известувања за

значителни или незначителни инциденти, сајбер закани и избегнати инциденти. MKD-GOV-CSIRT им дава приоритет на задолжителните пријави пред доброволните. Согласно член 38 став (5) од Законот, доброволното известување не создава дополнителни обврски за пријавителот. MKD-GOV-CSIRT ги проследува доброволните известувања до Министерството како единствена точка за контакт.

VI. ЗАВРШНИ ОДРЕДБИ

Член 34

Ова упатство се ревидира и ажурира по потреба, најмалку еднаш годишно, со цел да се усогласува со актуелните законски регулативи, оперативни практики и улогата на MKD-GOV-CSIRT.

Член 35

Ова Упатство влегува во сила со денот на потпишување од страна на Одговорното лице во Министерство за дигитална трансформација.

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