**20261392029**

## МИНИСТЕРСТВО ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА

Врз основа на член 25 став (11) од Законот за безбедност на мрежни и информациски системи (*) („Службен весник на Република Северна Македонија“ бр. 135/25), министерот за дигитална трансформација, донесе

# ПРАВИЛНИК ЗА ПОТРЕБНИТЕ СТРУЧНИ КВАЛИФИКАЦИИ, ОПШТИ И ПОСЕБНИ КОМПЕТЕНЦИИ ЗА ОФИЦЕР ЗА САЈБЕР БЕЗБЕДНОСТ ВО ИНСТИТУЦИИТЕ

Член 1

Со овој правилник се пропишуваат потребните стручни квалификации, општи и посебни компетенции за офицер за сајбер безбедност во Собранието на Република Северна Македонија, самостојните државни органи и регулаторните тела основани од Собранието на Република Северна Македонија, Владата на Република Северна Македонија, органите на државната управа, судовите, општините, општините во градот Скопје и градот Скопје.

Член 2

Овој правилник има за цел да ги пропише потребните професионални квалификации, општи и посебни компетенции за офицер за сајбер безбедност назначен во институции од јавниот сектор, што обезбедува офицерот за сајбер безбедност да поседува потребно експертско знаење и практично искуство за ефективно спроведување на мерки за сајбер безбедност, извршување на задолжителни задачи и усогласување на безбедносната позиција на институцијата со националните и меѓународните стандарди.

Член 3

Општи компетенции за офицер за сајбер безбедност се:

1) разбирање на националните и меѓународните правни рамки за сајбер безбедност;
2) способност за развој и имплементација на политики за сајбер безбедност;
3) способност за подготовка и имплементација на методологии за проценка на ризик и управување;
4) способност за следење и известување за усогласеност со прописите за сајбер безбедност;
5) познавање на мерките за безбедност на мрежи и информациски системи;
6) способност за откривање, анализа и одговор на инциденти;
7) способност за управување со ранливости и нивно надминување;
8) познавање на безбедност на податоци и криптографија;
9) познавање на безбедноста на ИКТ производи и услуги (вклучувајќи ги аспектите на ланецот на снабдување;
10) способност за внатрешна комуникација со засегнатите страни и
11) способност за надворешна координација.

Член 4

Разбирањето на националните и меѓународните правни рамки за сајбер безбедност опфаќа:

- напредно познавање на Законот за безбедност на мрежните и информациските системи (*), подзаконските акти кои произлегуваат од овој закон, како и Законот за заштита на личните податоци (*) и Законот за класифицирани информации (*);
- напредно познавање на релевантните директиви и регулативи за сајбер безбедност на Европската Унија и

- основно познавање за политиките и насоките на НАТО за сајбер безбедност, особено оние поврзани со заштита на критична инфраструктура и споделување информации.

Член 5

Способноста за развој и имплементација на политики за сајбер безбедност опфаќа:

- напредно ниво на способност за подготовка, имплементација и надзор на сеопфатна програма за сајбер безбедност, која вклучува развој на политики, процедури и мерки дизајнирани за заштита од сајбер-напади и зајакнување на сајбер отпорноста;
- напредно ниво на способност дефинирање на безбедносни политики за критични области како управување со ризик, контрола на пристап, енкрипција на податоци, континуитет на бизнисот и безбедна набавка, осигурувајќи дека овие политики се усогласени со организациските цели и законски барања и
- напредно ниво на способност за планирање и спроведување на сајбер одбраната на институцијата и на лидерски вештини.

Член 6

Способноста за подготовка и имплементација на методологии за проценка на ризик и управување опфаќа:

- напредно познавање од методологиите за проценка на ризик и управување и да има способност за идентификување на структурни и системски слабости и ризици низ информациски и комуникациски системи, мрежи, како и физичка и виртуелна инфраструктура;
- напредно ниво на способност за дефинирање сценарија и спроведување на проценки на ризик од сајбер безбедност како интегрален дел од сеопфатен систем за управување со ризик. Ова вклучува проценка на пропорционалноста на предложените безбедносни мерки врз основа на степенот на изложеност на ризици, веројатноста за инциденти и нивната потенцијална сериозност;
- напредно познавање на методологиите за проценка на ефикасноста на мерките за управување со ризици во сајбер безбедноста, вклучувајќи надзор на безбедносни ревизии и пенетраационо тестирање и
- напредно ниво на способност за техничка идентификација на ранливости и за квантитативно мерење и комуникација на ризикот во бизнис термини до менаџментот, овозможувајќи информирано донесување одлуки и оптимална распределба на ресурси.

Член 7

Способноста за следење и известување за усогласеност со прописите опфаќа:

- напредно ниво на способност за следење и обезбедување на соодветна примена на законски одредби, правилници и внатрешни акти поврзани со сајбер безбедноста, вклучувајќи компетенции во подготовка и активно учество во безбедносни ревизии и регулаторни проценки, обезбедувајќи континуирана усогласеност со воспоставените безбедносни политики и стандарди и
- напредно ниво на разбирање на обврските за заштита на личните податоци согласно Законот за заштита на личните податоци (*).

Член 8

Познавањето на мерките за безбедност на мрежи и информациски системи опфаќа:

- поседување на сеопфатно знаење за безбедносните мерки применливи на мрежни и информациски системи, спроведени на физичко, техничко и организациско ниво, кои се дизајнирани да се спротивстават на дејствија кои ја загрозуваат достапноста, автентичноста, интегритетот или доверливоста на податоците и
- способност за обезбедување на различни ИКТ производи, мрежи, инфраструктура и апликации, вклучувајќи ги и оние обезбедени од даватели на управувани услуги, како и познавање на вообичаени и стандардизирани практики, шеми за класификација и таксономии за ракување со инциденти и координирано откривање на ранливости.

Член 9

Способноста за откривање, анализа и одговор на инциденти опфаќа:

- напредно ниво на способност за откривање, анализа и одговор на инциденти, која вклучува редовно следење на ранливостите на системот, проценка на тековните закани за мрежните податоци и спроведување мерки за ублажување на последиците од сајбер инциденти;

- напредно ниво на способност да координира и учествува во мерките за заштита на системот за време на сајбер-напади и инциденти, што вклучува собирање и анализа на форензички податоци;

- напредно ниво на способност за навремено пријавување на значајни инциденти поврзани со сајбер безбедноста до надлежниот тим за одговор на компјутерски инциденти и

- напредно ниво на познавање на сеопфатните процедури за справување со инциденти (откривање, анализа, задржување, искоренување, опоравување) и управување со кризи.

Член 10

Способноста за управување со ранливости и нивно надминување опфаќа:

- напредни вештини за редовно следење на ранливостите на системот, што може да вклучува проактивно неинвазивно скенирање на јавно достапни системи и спроведување мерки за ублажување на идентификуваните последици и

- напредно ниво на способност за навремени и ефективни ажурирања на хардверските уреди и софтверските апликации, како и знаење за процеси на откривање, проценка и отстранување на ранливости.

Член 11

Познавањето на безбедност на податоци и криптографија опфаќа:

- средно ниво на разбирање и практична примена на политики и процедури за користење на криптографски техники и соодветна енкрипција за податоци, како во мирување така и во транзит и

- средно ниво на вештина во имплементација на робусни мерки за контрола на пристап, вклучувајќи мултифакторска автентикација (МФА) или решенија за континуирана автентикација, како и ефективно управување со безбедноста на човечките ресурси.

Член 12

Познавањето на безбедноста на ИКТ производи и услуги (вклучувајќи ги аспектите на ланецот на снабдување) опфаќа:

- средно ниво на познавања на безбедносните аспекти во текот на фазите на набавка, развој и одржување на мрежните и информациските системи;

- средно ниво на способност за процена и управување со ризиците од безбедноста во ланецот на снабдување, што вклучува евалуација на ранливости специфични за непосредни добавувачи и даватели на услуги, проценка на квалитетот на производите и внимателно следење на нивните практики за сајбер безбедност, како што се безбедните процеси на развој;

- напредно ниво на познавање на европските и меѓународните системи за сертификација на сајбер безбедност за ИКТ производи и услуги, како и способност да се обезбеди нивна употреба според барањата на Министерството за дигитална трансформација и

- средно ниво на способности за управување со добавувачи, преглед на договори и проценка на ризик.

Член 13

Способноста за внатрешна комуникација со засегнатите страни опфаќа:

- средно ниво на способност да комуницира ефективно и редовно со раководните лица и вработените во врска со прашања поврзани со сајбер безбедноста, вклучувајќи и преведување на сложени технички концепти во разбирлив деловен јазик;

- средно ниво на вештини за обезбедување редовна обука за управувачките тела и вработените за стекнување доволно знаење и вештини за идентификување ризици и проценка на мерките за сајбер безбедност и

- средно ниво на вештини за подготовка на предлози за специјализирана обука по сајбер безбедност за вработени во јавниот сектор и во развој на образовни програми насочени кон општа свест и сајбер хигиена.

Член 14

Способност за надворешна координација опфаќа:

- средно ниво на вештини за редовна комуникација и координација со надлежниот орган и надлежниот тим за одговор на инциденти со компјутерска безбедност;
- напредно ниво на познавање на националниот екосистем за сајбер безбедност, вклучувајќи ги различните улоги и одговорности на различни тимови за одговори на компјутерски инциденти, Единствената точка на контакт и механизмите за координација воспоставени за управување со големи инциденти и кризи и
- напредно ниво на способноста за соработка и размена на релевантни сајбер-безбедносни информации со други субјекти, вклучувајќи детали за сајбер закани, избегнати инциденти, ранливости и индикатори на компромитирање преку безбедни канали.

Член 15

Посебните компетенции претставуваат напредно знаење и специјализирани вештини кои значително ја подобруваат способноста на офицерот за сајбер безбедност да се справи со сложени и променливи сајбер закани.

Посебните компетенции се особено вредни за офицерите за сајбер безбедност кои работат во поголеми или покритични јавни институции, или за оние кои се стремат кон лидерски улоги во доменот на сајбер безбедноста, а вклучуваат:

- **Напредна анализа на закани и разузнавање**: Способноста за собирање, анализа и интерпретација на разузнавачки информации за сајбер закани од различни извори е клучна за предвидување и ефикасно спречување на сложени напади. Ова вклучува вештина во идентификување и профилирање на заканувачки актери, разбирање на нивните тактики, техники и процедури (TTP), како и развој на прилагодени одбранбени стратегии. Дополнително, вештини за спроведување проактивно, неинвазивно скенирање на јавно достапни мрежи и информациски системи за идентификување на ранливости и информирање на засегнатите субјекти.
- **Дигитална форензика и реконструкција на инциденти:** Експертиза во собирање, зачувување и анализа на форензички податоци по инцидент во сајбер-безбедноста е клучна за утврдување на основните причини, проценка на обемот и влијанието, како и поддршка на потенцијални правни постапки, како и способноста за поддршка на истраги на истражните органи кога се сомнева на кривично дело поврзано со значаен сајбер-безбедносен инцидент.
- **Архитектура и дизајн на безбедноста**: Офицерот за сајбер безбедност треба да има способност да планира и изготвува безбедносни решенија, осигурувајќи дека контролите на сајбер безбедноста се интегрирани и во новите и во постоечките информациски и комуникациски системи и мрежи од нивното основање. Ова вклучува темелно разбирање на принципите и практиките на животниот циклус на безбеден развој на системи (SSDLC) во однос на набавката, развојот и одржувањето на мрежни и информациски системи.
- **Континуитет на бизнисот и планирање на обновување од катастрофи**: Напредните вештини за развој, имплементација и тестирање на сеопфатни планови за континуитет на бизнисот се клучни. Ова вклучува структурно и системско управување со резервни копии, ефективни стратегии за обновување по катастрофи и добро дефинирани протоколи за управување со кризи. Офицерот за сајбер безбедност мора да може да обезбеди континуитет и отпорност на важни услуги дури и во случај на значајни инциденти со сајбер безбедност или големи сајбер кризи.
- **Облачна безбедност и нови технологии**: Разбирањето на безбедносните импликации, ризици и најдобрите практики поврзани со компјутерски услуги во облак, управувани услуги и други нови дигитални технологии станува сè поважно. Офицерот за

сајбер безбедност мора да биде способен да ги проценува и управува ризиците од сајбер-безбедноста поврзани со усвојувањето и употребата на нови технологии и дигитални средини во јавниот сектор.

- **Безбедносна ревизија и надзор на пенетрациско тестирање**: Компетентноста во надзор или спроведување безбедносни ревизии и пенетрациски тестирања е неопходна за објективна проценка на ефикасноста на мерките за управување со ризик од сајбер безбедност. Ова исто така вклучува можност за прецизно толкување на резултатите од ревизијата, идентификување на области на неусогласеност и препорака на соодветни корективни мерки и подобрувања.

Член 16

Компетенциите за сајбер безбедност се подобруваат со стекнување на меѓународен сертификати од следните области:

- општи познавања на сајбер безбедноста;
- управување, ризик и усогласеност;
- одговор на компјутерски инциденти и дигитална форензика;
- архитектура и инженеринг на сајбер безбедноста;
- безбедност во облак;
- управување со ранливости и тестирање на пенетрација и/или
- усогласеност со НИС2.

Министерството за дигитална трансформација објавува индикативна листа на меѓународните сертификати од ставот 1 на овој член, како и нивните издавачи.

Член 17

Овој правилник влегува во сила наредниот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 10-1450/1
23 јуни 2026 година
Скопје

Министер за дигитална
трансформација,
**Стефан Андоновски с.**р.