20261281843

МИНИСТЕРСТВО ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА

Врз основа на член 46 став (6) 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 ФОРМАТА И СОДРЖИНАТА НА ОБРАЗЕЦОТ НА ЗАПИСНИКОТ ЗА ИЗВРШЕН СТРУЧЕН НАДЗОР

Член 1

Со овој правилник се пропишува формата и содржината на образецот на записникот за извршен стручен надзор.

Член 2

(1) Записникот за извршен стручен надзор се изготвува на образец испечатен на хартија во бела боја, во А4 формат.

(2) По исклучок од ставот (1) на овој член, записник може да се изготви и во електронска форма кога за тоа постојат соодветни технички услови согласно прописите од областа на електронските документи и доверливи услуги.

(3) Содржината на образецот на записникот за извршен стручен надзор е дадена во Прилог, кој е составен дел на овој правилник.

Член 3

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

Бр. 10-1352/1
9 јуни 2026 година
Скопје

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

ПРИЛОГ

МИНИСТЕРСТВО ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА

Записник за извршен стручен надзор

Број _____

Датум _____

1. **Податоци за субјектот на стручниот надзор**

Назив на субјектот на надзорот: _____;

Седиште на субјектот на надзорот: _____ ;

Електронска адреса на субјектот на надзорот: _____;

Телефон на субјектот на надзорот: _____;

Матичен број на субјектот на надзорот: _____ ;

Даночен број на субјектот на надзорот: _____ ;

Овластено лице кај субјектот на надзорот:

Име и презиме _____;

Живеалиште _____;

Телефонски број _____;

Електронска адреса _____;

2. **Податоци за стручниот надзор**

1) Редовен
2) Вонреден

Чекор	Барање	Опис	Суштински субјект	Важен субјект	Исполнува (Да или Не)	Образложение
Анализа на безбедност на ризик и информациски системи	1.1. Дефинирање на опсег и цели	Дефинирајте го опсегот и целите на проценката на ризикот, идентификувајќи кои системи, мрежи и бизнис процеси се вклучени, во согласност со бизнис целите.	З	П		
	1.2. Идентификација и класификација на средства	Креирајте и одржувајте сеопфатен инвентар на сите критични ИТ средства, класифицирајќи ги според вредност и деловна критичност.	З	З		
	1.3. Идентификација на закани и ранливости	Активно идентификувајте потенцијални внатрешни и надворешни закани и ранливости користејќи	З	З		

		рамки како MITRE ATT &CK.				
	1.4. Анализа на ризик	За секој идентификуван ризик, проценете ја веројатноста и потенцијалното влијание врз доверливоста, интегритетот и достапноста користејќи матрица на ризик или модел базиран на податоци.	З	З		
	1.5. План за третман на ризик	Развијте и документирајте конкретен, остварлив план за справување со ризици со висок приоритет, со доделени сопственици и рокови.	З	П		
	1.6. Имплементација на безбедносна контрола	Воведете и превентивни и детективски безбедносни контроли за намалување на ризиците.	З	З		
	1.7. Континуир	Воспоставете процес за континуирано	З	П		

	ано следење	следење на безбедносната состојба, вклучувајќи редовни скенирања на ранливости.				
	1.8. Редовен преглед и одобрување	Спроведувајте и одобрувајте проценки на ризик најмалку еднаш годишно и по значајни промени во ИТ средината.	3	3		
	1.9. Комуникација со засегнатите страни	Комуницирајте ги резултатите од проценката и плановите за санација до високиот менаџмент и клучните засегнати страни, прилагодувајќи ги извештаите на публиката.	3	3		
	1.10. Документација	Документирајте го целиот процес на проценка на ризикот, вклучувајќи методологии, идентификувани ризици и имплементирани контроли.	3	3		

Ракување со инциденти	2.1. Подготовка и одобрување на план	Развијте формален, писмен План за одговор на инциденти (IRP) со јасна мисија и дефинирани улоги, формално одобрени од високото раководство.	3	3		
	2.2. Безбедна комуникација	Воспоставете безбеден комуникациски канал за тимот за одговор на инциденти кој е одделен од нормалните, потенцијално компромитирани системи.	3	3		
	2.3. Детекција и анализа	Имплементирајте алатки и процедури за следење на мрежата, анализа на аларми и разликување меѓу безбедносни настани и инциденти.	3	3		
	2.4. Пријавување на	Веднаш, и најдоцна три часа по	3	3		

	инцидент и (задолжително)	дознавањето, известете го компетентниот CSIRT за било каков значаен инцидент или закана.				
	2.5. Навремено известување и финален извештај	Да се обезбеди рано предупредување во рок од 24 часа од значаен инцидент и детален извештај во рок од 72 часа. Конечниот извештај мора да биде доставен во рок од еден месец од решавањето.	3	3		
	2.6. Задржување	Спроведете краткорочни и долгорочни мерки за ограничување за да спречите ширење на инцидент, како што е изолирање на погодените системи.	3	3		
	2.7. Искоренување	Целосно отстранете ја заканата од	3	3		

		сите погодени системи. Ова вклучува отстранување на малициозен софтвер и поправка на ранливости.				
	2.8. Опоравување	Вратете ги засегнатите системи во нормална работа користејќи тестирани резервни копии.	З	З		
	2.9. Преглед по инцидент от	Спроведете формален преглед по инцидентот за да го утврдите коренот на причината, идентификувајте што поминало добро и да ги документирате научените лекции.	З	З		
	2.10. Прирачници и вежби	Развивајте и одржувајте прирачници за одговор на инциденти за вообичаени закани и спроведувајте	З	П		

		редовни вежби и вежби на маса.				
Континуитет на бизнисот, обновување по катастрофи и управување со кризи	3.1. Анализа на влијанието врз бизнисот (BIA)	Спроведете BIA за да ги идентификувате и приоритизирате основните деловни функции и нивните поддржувачки ИТ системи.	3	3		
	3.2. Цели за опоравување	Воспоставете јасни Цели за време на опоравување (RTOs) и Цели на точки за опоравување (RPO) за секој критичен ресурс.	3	3		
	3.3. Управување со резервни копии	Имплементирајте робустна стратегија за резервни копии со редовни, непроменливи и гео-разновидни резервни копии за сите критични податоци и системи.	3	3		

	3.4. План за обновување по катастрофа	Развијте и одржувајте писмен план за обновување по катастрофа кој вклучува детални процедури за обновување и редовно се ажурира.	З	З		
	3.5. План за управување со кризи	Креирајте посебен план за управување со кризи за нетехнички аспекти на голем настан, вклучувајќи стратегии за комуникација.	З	П		
	3.6. Тестирање на планови	Спроведувајте редовни, документирани тестови на плановите за обновување по катастрофи и континуитет на бизнисот.	З	П		
	3.7. Комуникациски план	Осигурајте се дека комуникацискиот план вклучува протоколи за користење безбедни, алтернативни	З	З		

		канали во случај на дефект на мрежата.				
	3.8. Инвентар на средства	Одржувајте детална евиденција на целиот хардвер, софтвер и податоци, како и нивните конфигурации и меѓузависности.	З	З		
	3.9. Преглед по катастрофата	По секоја катастрофа или голем тест, спроведете формален преглед за анализа на одговорот и ажурирање на планот за идни настани.	З	З		
	3.10. Обука на вработени	Осигурајте се дека сите релевантни вработени се обучени за нивните улоги и одговорности во рамките на плановите за континуитет на бизнисот и	З	П		

		обновување од катастрофи.				
Безбедност на синџирот на снабдување	4.1. Управување и одобрување	Назначете старши лидер за безбедност на синџирот на снабдување и имајте формална политика одобрена од високото раководство.	З	П		
	4.2. Регистар на ризици	Осигурајте се дека ризиците од синџирот на снабдување формално се евидентирани во регистарот на ризици на организацијата за видливост на високо ниво.	З	П		
	4.3. Длабинска проверка на добавувачи	Спроведете темелна безбедносна проверка на сите потенцијални добавувачи пред да склучите договор, намалувајќи го бројот на добавувачи за да го	З	П		

		поедноставите надзорот на ризикот.				
	4.4. Договорни клаузули	Спроведување на безбедносните очекувања преку вклучување на соодветни клаузули за сајбер безбедност во сите договори со добавувачите.	З	З		
	4.5. Минимални безбедносни стандарди	Дефинирање и спроведување минимален стандард за сајбер безбедност за сите добавувачи, усогласен со призната рамка од трета страна.	З	З		
	4.6. Континуирано следење	Редовно следете ја усогласеноста на добавувачите со безбедносните стандарди преку ревизии, безбедносни	З	П		

		прашалници и стрес тестови.				
	4.7. Споделување информации	Промовирајте отворено пријавување на безбедносни инциденти од добавувачи и споделете релевантни разузнавачки информации за закани.	З	П		
	4.8. Ревизии	За добавувачите со висок ризик, спроведувајте редовни безбедносни ревизии и прегледајте ја нивната безбедносна состојба.	З	П		
	4.9. Соработка при одговор на инциденти	Бидете подготвени да обезбедите поддршка и помош на добавувачите за време на безбедносен инцидент.	З	П		
	4.10. Процедури за	Воспоставете формални процедури за безбедно повторно	З	З		

	раскинување	враќање на контролата врз вашите средства и одземање пристап од добавувачите на крајот од договорот.				
Безбедност во набавката, развојот и одржувањето	5.1. Безбеден дизајн	Интегрирајте безбедносни барања и моделирање на закани во почетните фази на планирање и дизајн на нови системи.	3	3		
	5.2. Безбедно кодирање	Следете безбедни практики за кодирање, користете статички и динамички алатки за анализа и спроведувајте редовни прегледи на кодот.	3	3		
	5.3. Управување со ранливости	Воспоставете формална, документирана политика за управување со ранливости за систематско идентификува	3	3		

		ње, евалуација и адресирање на безбедносните слабости.				
	5.4. Редовно скенирање на ранливости	Редовно скенирајте ранливости на сите мрежни системи и апликации за да ги идентификувате слабостите и погрешните конфигурации.	3	3		
	5.5. Управување со закрпи	Имплементирајте робустен систем за управување со закрпи за брзо применување на безбедносни закрпи и ажурирања.	3	3		
	5.6. Безбедно распоредување	Следете ги практиките за безбедно распоредување, вклучувајќи спроведување безбедносни проценки на средината за распоредување.	3	3		

	5.7. Сертифицирани производи	Користете ИКТ услуги, системи и производи кои се сертифицирани според европски и меѓународни шеми за сертификација на сајбер безбедност каде што се достапни.	З	П		
	5.8. Безбедно одржување	Континуирано давајте приоритет на безбедноста за време на фазата на одржување преку следење на нови ранливости и системи за ажурирање.	З	З		
	5.9. Интеграција на разузнавачки информации за закани	Користете разузнавачки информации за закани за да идентификувате трендови и шеми кои можат да укажуваат на идно безбедносно прекршување.	З	П		

	5.10. Редовен преглед и одобрување	Редовно прегледувајте и ажурирајте политики поврзани со набавка, развој и одржување, со формално одобрување од менаџментот.	З	З		
Политики и процедури за проценка на ефикасноста	6.1. Усвојете рамка	Усогласете ги безбедносните практики со призната рамка како NIST, ISO/IEC 27001 или CIS Controls.	З	П		
	6.2. Документација на политики и процедури	Креирајте јасни, лесни за читање и редовно ажурирани политики и процедури за сајбер безбедност, формално одобрени од високиот менаџмент.	З	З		
	6.3. Годишни безбедносни ревизии	Спроведете формални, независни безбедносни ревизии најмалку еднаш годишно за споредба на	З	П		

		политиките за сајбер безбедност на организацијата со нејзините реални практики.				
	6.4. Таргетирани ревизии	Бидете подготвени да спроведете таргетирани безбедносни ревизии кога ќе биде побарано од надлежниот орган.	З	П		
	6.5. Континуирано следење	Имплементирајте систем за управување со безбедносни информации и настани (SIEM) за континуирано следење на мрежната активност и однесувањето на корисниците.	З	П		
	6.6. Евидентирање на инциденти и настани	Осигурајте се дека сите безбедносни инциденти и системски настани се правилно евидентирани	З	З		

		и одржувани во одреден период за форензичка анализа.				
	6.7. Следење на санација	Имплементирајте систем за следење на отстранувањето на сите идентификувани ранливости и погрешни конфигурации.	З	П		
	6.8. Ревизија и преглед на политики	Периодично ревидирајте ги политиките и процедурите за сајбер безбедност за да се осигурате дека сè уште се релевантни и ефективни.	З	О		
	6.9. Анализа на ризик	Редовно преиспитувајте ја толеранцијата на ризик и потенцијалното влијание од безбедносните пробиви за да се усогласи распределбата на ресурсите со деловните цели.	З	О		

	6.10. Надворешни скенирања	Спроведете проактивно, неинвазивно скенирање на јавно достапни мрежни и информациски системи за идентификување на ранливости.	З	О		
Основна хигиена и обука за сајбер безбедност	7.1. Задолжителна програма за обука	Воведете задолжителна, континуирана програма за обука за безбедност за сите вработени и изведувачи, најмалку годишно.	З	З		
	7.2. Теми за обука	Обуката треба да опфати фишинг, социјално инженерство, малициозен софтвер, управување со лозинки и безбедна употреба на преносливи уреди.	З	З		
	7.3. Политика за силна лозинка	Спроведете политика за силна лозинка која налага комплексност,	З	З		

		забранува повторна употреба и бара редовна ротација на лозинки.				
	7.4. Фишинг заштита	Имплементирајте и обезбедувајте обука за користење на алатки и процедури против фишинг.	3	3		
	7.5. Политика за користење на уреди	Креирајте јасни, документирани политики за користење на лични уреди за работа и уреди издадени од компанијата за лични активности.	3	3		
	7.6. Редовни ажурирања и закрпи	Осигурајте се дека целиот софтвер и оперативни системи се ажурираат редовно и дека безбедносните закрпи се применуваат навремено.	3	3		

	7.7. Обука за пријавување инциденти	Обучете ги сите вработени како веднаш да идентификуваат и пријават сомнителни активности или потенцијални безбедносни инциденти.	3	3		
	7.8. Политики за контрола на пристап	Обучувајте ги вработените според принципот на најмала привилегија и други политики за контрола на пристап.	3	3		
	7.9. Воведување/Отстранување на вработени	Интегрирајте ја свесноста за сајбер безбедност во воведувањето и обезбедите навремено одземање на пристапот за време на откажувањето.	3	3		
	7.10. Редовен преглед и одобрување	Сите политики и програми за обука мора да се прегледуваат и формално одобруваат најмалку	3	3		

		еднаш годишно.				
Употреба на криптографски техники и енкрипција	8.1. Класификација на податоци	Класифицирајте ги податоците според чувствителност и применете соодветна енкрипција според нивната критичност.	3	3		
	8.2. Енкрипција на податоци во мирување	Користете целосно шифрирање на дискот за сите уреди и медиуми кои чуваат чувствителни или класифицирани податоци.	3	3		
	8.3. Енкрипција на податоци во транзит	Шифрирање на податоци пренесени преку јавни мрежи користејќи безбедни протоколи како TLS 1.3, IPsec или S/MIME.	3	3		
	8.4. Политика за управување	Имплементирајте формална, одобрена политика за управување со	3	3		

	е со клучеви	клучеви која го опфаќа целиот животен циклус на криптографски те клучеви.				
	8.5. Употреба на силни алгоритми	Задолжително користење на модерни, одобрени алгоритми како AES-256 и RSA (минимум 2048-битна должина на клуч), и забрани застарени алгоритми како DES или RC4.	З	З		
	8.6. Безбедно складирање на клучеви	Чуваат криптографски клучеви безбедно, одделени од апликацискиот код, користејќи HSM или облачно базирани KMS.	З	О		
	8.7. Ротација на клучеви	Имплементирајте распоред за периодична ротација на клучот за да го минимизирате влијанието на компромитиран клуч.	З	З		

	8.8. Енкрипција од крај до крај	Каде што е можно, имплементирајте end-to-end енкрипција за да спречите посредници да пристапуваат до податоците.	З	О		
	8.9. Враќање на клучеви	Осигурајте се дека има можност за опоравување на податоци во случај да се изгуби или оштети енкрипциски клуч.	З	З		
	8.10. Логирање и ревизија	Евидентирајте ги сите активности поврзани со клучеви за ревизија и имплементирајте контроли на пристап.	З	З		
Безбедност на човечките ресурси, политики за контрола на пристап и управување со средства	9.1. Политика за животен циклус на безбедност на човечки ресурси	Спроведете сеопфатна политика за сајбер безбедност во HR која ги адресира безбедносните барања пред, за време и по завршувањето	З	З		

		на работното место, со формално одобрување од менаџментот.				
	9.2. Безбедносна проверка	Спроведете безбедносни проверки за сите лица кои ќе имаат привилегиран пристап до критични системи и чувствителни податоци.	З	О		
	9.3. Улоги и одговорности	Јасно дефинирајте ги улогите и одговорностите во сајбер безбедноста во описите на работните места и нека персоналот формално се согласи со своите обврски.	З	З		
	9.4. Политика за контрола на пристап	Спроведете принцип на најмала привилегија (PoLP), обезбедувајќи корисниците да имаат само минимален	З	З		

		пристап потребен за нивните работни функции.				
	9.5. Одземање на пристап	Воведете процедури за веднаш повлекување на сите права на пристап до мрежата и системот при отпуштање или промена на улогата на вработениот.	3	3		
	9.6. Сеопфатен инвентар на средства	Креирајте и одржувајте детална, ажурирана инвентар на сите ИТ средства користејќи повеќе методи за откривање за точност.	3	3		
	9.7. Класификација на средства	Класифицирајте ги сите средства врз основа на нивната бизнис критичност, вредност и чувствителност за да ги приоритизирате	3	3		

		управувачките и безбедносните напори.				
	9.8. Управување со животен циклус на средства	Имплементирајте систем за следење на средствата низ целиот нивен животен циклус, од набавка до отстранување.	З	П		
	9.9. Редовни ревизии на пристап	Спроведувајте редовни ревизии на корисничките сметки и пристапни права за идентификација и отстранување на застарени или непотребни привилегии.	З	З		
	9.10. Безбедно отстранување	Следете безбедни и еколошки одговорни процедури за отстранување на средства, вклучувајќи отстранување на сите податоци од хардверот.	З	З		

Употреба на мултифакторска автентикација (MFA) и безбедни комуникациски системи	10.1. MFA за привилегирани сметки	Задолжително користење на мултифакторска автентикација за сите привилегирани или административни сметки.	З	З		
	10.2. MFA за далечински пристап	Барајте MFA за сите конекции за далечински пристап, вклучувајќи VPN и услуги за далечински десктоп.	З	З		
	10.3. MFA за е-пошта и облачни услуги	Спроведете MFA за пристап до корпоративна е-пошта, облачни апликации и системи за складирање датотеки.	З	П		
	10.4. Користење на MFA отпорен на фишинг	Имплементирајте и поттикнете употреба на MFA методи отпорни на фишинг, како што се FIDO безбедносни клучеви или паметни картички.	З	П		

	10.5. Адаптивна автентикација	Имплементирајте адаптивни решенија за автентикација кои динамично ги зголемуваат или намалуваат чекорите за автентикација врз основа на контекстуални информации.	З	П		
	10.6. Безбеден глас, видео и текст	Осигурајте се дека внатрешната гласовна, видео и текстуална комуникација е заштитена со соодветна енкрипција.	З	П		
	10.7. Безбедна итна комуникација	Воспоставете и одржувајте безбеден систем за итна комуникација кој не се потпира на јавни мрежи.	З	З		
	10.8. Политика за внатрешна комуникација	Развијте и спроведете формална, одобрена политика која ќе одреди кои комуникациски канали се	З	З		

		одобрени за различни типови информации.				
	10.9. Обука на вработени	Едуцирајте ги сите вработени за важноста на MFA и правилната употреба на безбедни комуникациски системи.	3	3		
	10.10. Континуирано следење	Континуирано следете ги сите логови за автентикација и комуникација за да откриете сомнителни активности и потенцијални компромитирања.	3	3		

3. Податоци за овластеното/ите лица кој/и го извршил/е стручниот надзор

Стручниот надзор е извршен од:

1. _____ со број на легитимација _____;
2. _____ со број на легитимација _____;
3. _____ со број на легитимација _____;
4. _____ со број на легитимација _____;

4. Податоци за претставникот/ците на субјектот на стручниот надзор

На стручниот надзор присуствуваа:

1. _____ со работно место _____;
2. _____ со работно место _____;
3. _____ со работно место _____;
4. _____ со работно место _____;

5. **Информација за презентирањето на записникот пред претставникот на субјектот на стручниот надзор;**

Со содржината на записникот беа запознаени присутните лица на надзорот:

1) ДА
3) НЕ

6. **Забелешки на субјектот на стручниот надзор**

Претставниците на субјектот на стручниот надзор ги дадоа следните забелешки:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Датум, име, презиме и потпис на претставникот на субјектот на стручниот надзор:

- Датум _____;
- Име и презиме _____;
- своерачен потпис _____;

Место: _____;

Датум: _____;

Потпис на овластено лице за стручен надзор и печат: _____