Република Северна Македонија
Republika e Maqedonisë së Veriut
Министерство за дигитална трансформација
Ministria e transformimit dixhital
Бр. - Nr 10-1344/1
09.06.2026 год. - viti
Скопје / Shkup

Врз основа на член 32 став (8) 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 УТВРДУВАЊЕ НА ТЕХНИЧКИ И МЕТОДОЛОШКИ БАРАЊА ЗА МЕРКИ ЗА УПРАВУВАЊЕ СО РИЗИЦИТЕ КОИ ПРЕТСТАВУВААТ ЗАКАНА ЗА МРЕЖНИТЕ И ИНФОРМАЦИСКИТЕ СИСТЕМИ

Предмет
Член 1

Со овој правилник се утврдуваат техничките и методолошките барања за мерки за управување со ризиците кои претставуваат закана за мрежните и информациските системи во Владата, министерствата, самостојните органи на државната управа, органите на државната управа во состав на министерствата, управните организации, општините, општините во градот Скопје и градот Скопје.

Анализа на ризиците за безбедност на мрежните и информациските системи
Член 2

Прв чекор за управување со ризиците кои претставуваат закана за мрежните и информациските системи е анализата на ризиците за безбедност на мрежните и информациските системи.

Оваа мерка опфаќа систематско идентификување, евалуација и приоритизирање на ризиците од сајбер безбедноста за мрежните и информациските системи на субјектот.

Анализата на ризици потребно е да биде континуиран процес, интегриран во стратешкото и оперативното планирање на субјектот се со цел безбедносната состојба да остане актуелна и релевантна.

Анализата на ризици опфаќа:

- Дефинирање на обем и цели: Субјектите се должни да го дефинираат обемот и целите на нивната анализа на ризици, идентификувајќи кои системи, мрежи и работните процеси се вклучени. Овој процес треба да биде поврзан со работните целите на субјектот за да се осигура дека проценката е релевантна и фокусирана на она што е најважно за функционирањето.
- Идентификација и класификација на средства: Потребно е да се создаде и одржува сеопфатен попис на сите критични ИТ средства, вклучувајќи хардвер, софтвер, податоци и мрежни компоненти. Средствата треба да се класифицираат според критичноста, вредноста и чувствителноста на работата за да се приоритизираат управувачките напори.
- Идентификација на закани и ранливости: Субјектот мора активно да ги идентификува потенцијалните внатрешни и надворешни закани и ранливости.

Се препорачува користење на воспоставени рамки како MITRE ATT&CK и Националната база на ранливости за сеопфатно разбирање на потенцијалните вектори и слабости на нападите.

- Анализа на ризици: Потребно е да се изврши детална анализа на ризици за да се процени веројатноста заканата да ја искористи ранливоста и потенцијалното влијание врз доверливоста, интегритетот и достапноста. Матрица на ризик или модел за квантитативна проценка базиран на податоци треба да се користи за оценување и приоритизирање на ризиците врз основа на работната вредност, а не само според техничката сериозност.
- План за справување со ризици: Субјектот е должен да развие документиран план за справување со ризици со висок приоритет. Планот може да вклучува ублажување, прифаќање, избегнување или пренос на ризик. Планот мора да биде конкретен, остварлив и да содржи податоци за одговорна страна, временска рамка и индикатори и критериуми за реализација на секоја препорака.
- Имплементација на безбедносна контрола: Субјектите се должни да имплементираат безбедносни контроли, како заштитни ѕидови, контроли на пристап и енкрипција, за да ги намалат идентификуваните ризици. Имплементацијата треба да вклучува и превентивни и тековни контроли.
- Континуирано следење: Субјектите се должни да воспостават процес за континуирано следење на безбедносната состојба, вклучувајќи редовни скенирања на ранливости и тестирање на пенетрација, со цел да се обезбеди континуирана ефективност на воспоставените контроли и навремено идентификување на новонастанати ранливости кога ќе се појават.
- Редовен преглед и одобрување: Раководните лица на субјектите се должни да спроведуваат проценка на ризици најмалку еднаш годишно и да ги одобрат мерките за управување со ризици, со што се обезбедува политиките и процедурите редовно да се прегледуваат и ажурираат се со цел да се одговори на новите закани и промените во работењето на субјектот.
- Комуникација со засегнатите страни: Субјектите се должни да обезбедат соодветна и навремена комуникација на резултатите од проценката и плановите за справување со ризици со раководните лица во субјектите и клучните засегнати страни. Извештаите треба да бидат прилагодени на потребите и компетенциите на оние на кои се доставуваат, претварајќи ги техничките наоди во разбирливи податоци за влијание на ризиците врз работата на субјектите и овозможувајќи им на раководните лица да донесуваат соодветни одлуки за толеранцијата на ризиците.
- Документирање: Субјектите се должни да го документираат целиот процес на проценка на ризици, вклучувајќи методологии, идентификувани ризици и имплементирани контроли. Оваа документација служи како клучна заштита за време на ревизија и обезбедува јасен запис за континуирано подобрување.

Управување со инциденти

Член 3

Втор чекор за управување со ризиците кои претставуваат закана за мрежните и информациските системи е воспоставување на структуриран и проактивен пристап за управување и одговор на сајбер безбедносни инциденти, со цел да се минимизира влијанието од нападот и да се обезбеди брзо закрепнување на погодените системи и услуги.

Процесот на управување со инциденти мора да следи структуриран, повеќефазен животен циклус за да биде ефикасен и опфаќа:

- Подготовка и одобрување на планот: Субјектот е должен да развие формален, писмен План за одговор на инциденти (IRP) со јасна мисија и дефинирани улоги за крос-функционален тим за одговор на инциденти. IRP мора формално да биде одобрен од раководното лице на субјектот за да се обезбеди усогласеност со работните цели и да се обезбедат потребните ресурси.
- Безбедна комуникација: Субјектот е должен да воспостави безбеден комуникациски канал кој е одделен од вообичаените, потенцијално компромитирани системи за тимот за одговор на инциденти. Овој канал треба да обезбеди непречена, доверлива и сигурна комуникација во услови на инцидент или кризна состојба, со цел зачувување на доверливоста и интегритетот на разменетите информации за време на процесот на одговор.
- Детекција и анализа: Субјектите се должни да имплементираат алатки (на пр., SIEM, IDS/IPS) и процедури за следење на мрежата, анализа на аларми и разликување на безбедносни настани и инциденти. Процесот на ескалација треба да се дефинира со приоритет на значајните закани.
- Пријавување на инциденти Субјектите се должни веднаш, а најдоцна во рок од три часа од моментот на дознавање за настанувањето на инцидентот или заканата, да го известат надлежниот Тим за одговор на компјутерски безбедносни инциденти за секој значаен сајбер безбедносен инцидент или сајбер закана.
- Навремено известување и конечен извештај: Субјектите се должни до надлежниот Тим за одговор на компјутерски безбедносни инциденти да достават рано предупредување во рок од 24 часа од дознавањето за зазначаен сајбер безбедносен инцидент, а детален извештај мора да се достави во рок од 72 часа, вклучувајќи и почетна проценка на сериозноста и влијанието на инцидентот. Субјектите се должни да достават конечен извештај во рок од еден месец по решавањето на сајбер безбедносниот инцидент.
- Спречување: Субјектите се должни да спроведат краткорочни и долгорочни мерки за зспречување со цел да се спречи ширење на инцидентот, како што

е изолирање на погодени системи или сегментирање на мрежата.

- Отстранување: Заканата мора целосно да се отстрани од сите погодени системи. Ова вклучува отстранување на малициозен софтвер, поправка на ранливости и ресетирање на компромитирани кредендијали.
- Оправување: Субјектите се должни да ги вратат засегнатите системи во состојба на нормална работа со користење на тестирани резервни копии, на посебна мрежа за тестирање, надвор од мрежата на субјектот. Пред повторно ставање во функција, субјектите се должни да потврдат дека сите системи се целосно функционални и безбедни.
- Преглед по инцидентот: По инцидентот субјектите се должни да спроведат формален преглед за да се утврди изворот на причината за настанување на инцидентот, да се идентификуваат позитивните аспекти при справување со инцидентот и да се документираат научените лекции за да се спречат идни инциденти. Овој преглед треба да вклучува формална евалуација за подобрување на системите, алатките и процесите.
- Прирачници и вежби: Субјектите се должни да развијат и одржуваат прирачници за одговор на инциденти за вообичаени закани и да спроведуваат редовни дискусии и практични вежби за да ја тестираат ефикасноста на Планот за одговор на инциденти. Сите документи и белешки потребно е внимателно да се чуваат за форензичка анализа и идни референци.

Континуитет на работењето, обновување од катастрофи и управување со кризи

Член 4

Трет чекор за управување со ризиците кои претставуваат закана за мрежните и информациските системи е обезбедување на континуитет на работењето на субјектот, обновување од катастрофи и управување со кризи.

Овој чекор се фокусира на мерките и плановите потребни за обезбедување на континуитет на критичните услуги и операции со минимални нарушувања во случај на значаен сајбер напад или катастрофа, и опфаќа:

- Анализа на влијание врз работата на субјектот (BIA): Субјектите се должни да спроведат анализа на работата на субјектот за да ги идентификуваат и приоритизираат основните деловни функции и поддржувачките ИТ системи, податоци и апликации кои прво мора да се вратат. Анализата на работата треба да вклучи мислења од сите организациски единици на субјектот.
- Цели за оправување: Јасни временски цели (RTOs) и цели на точки за оправување (RPO) мора да се утврдат за секој критичен ресурс. Целите на точките за оправување ја одредуваат резервната фреквенција, додека јасните временски цели го дефинираат максимално прифатливото време на

застој.

- Управување со резервни копии: Мора да се имплементира робусна стратегија за резервни копии за сите критични податоци и системи. Субјектите се должни да се осигураат дека резервните копии се прават редовно, и дека се користат непроменливи резервни копии кои се чуваат во различни региони, а заради заштита од рансомвер и регионални катастрофи.
- План за обновување од катастрофа: Субјектите се должни да развијат и одржуваат писмен план за обновување по катастрофа, вклучувајќи детални процедури за обновување на системите, план за комуникација со контакти за итни случаи и листа на сите критични средства. Планот мора редовно да се ажурира секогаш кога организациската структура, инфраструктурата или апликациите на субјектот се менуваат.
- План за управување со кризи: Субјектите се должни да развијат посебен план за управување со кризи за нетехнички аспекти на голем настан, вклучувајќи комуникациски стратегии за засегнатите страни, медиумите и засегнатите корисници.
- Тестирање на планови: Субјектите се должни да спроведуваат редовни, документирани тестови на плановите за обновување по катастрофа и континуитет на работните процеси. Ова може да вклучува симулациски вежби за идентификување празнини и обезбедување на изводливоста на планот.
- Комуникациски план: Комуникацискиот план задолжително вклучува протоколи за користење безбедни и алтернативни канали во случај на дефект на мрежата. Ова е од суштинско значење со цел да се обезбеди непречена комуникација дури и кога примарните мрежи се исклучени.
- Попис на средства: Субјектите се должни да одржуваат листа со детален попис на целиот критичен хардвер, софтвер и податоци, како и на нивните конфигурации и меѓузависности, за да се овозможи брзо закрепнување.
- Преглед по катастрофа: По секоја катастрофа или голем тест, субјектите се должни да спроведат формален преглед за анализа на одговорот, документирање на научените лекции и ажурирање на планот за идни настани и инциденти.
- Обука на вработените: Сите релевантни вработени мора да бидат обучени за нивните улоги и одговорности во рамките на плановите за континуитет на работните процеси и обновување од катастрофи.

Безбедност на ланецот на снабдување

Член 5

Четврт чекор за управување со ризиците кои претставуваат закана за мрежните и информациските системи е безбедност на ланецот на снабдување.

Овој чекор се занимава со управување и ублажување на ризиците од сајбер безбедноста предизвикани од трети страни добавувачи, добавувачи и даватели на услуги и опфаќа:

- Управување и одобрување: Мора да се назначи одговорно лице за безбедноста на ланецот на снабдување. Тимовите за набавка и безбедност треба да бидат интегрирани за да се обезбеди холистички пристап кон управувањето со ризици. Политиката за безбедност на ланецот на снабдување мора формално да биде одобрена од раководното лице на субјектот.
- Регистар на ризици: Ризиците во ланецот на снабдување мора формално да се регистрираат во централниот регистар на ризици на субјектот за видливост на високо ниво.
- Длабинска проверка на добавувачите: Мора да се спроведе темелна безбедносна проверка на сите потенцијални добавувачи и даватели на услуги пред склучување договор. Бројот на добавувачи треба да се намали за да се поедностави управувањето и надзорот на ризикот.
- Договорни клаузули: Безбедносните очекувања мора да се спроведуваат со вклучување на соодветни клаузули за сајбер безбедност во сите договори со добавувачи. Овие клаузули треба да бараат безбедносни стандарди и усогласеност со законските барања.
- Минимални безбедносни стандарди: Мора да се дефинира и спроведе минимален стандард за сајбер безбедност за сите добавувачи, усогласен со призната рамка од трета страна, за да се обезбеди дека сите работат според истите правила.
- Континуирано следење: Усогласеноста на добавувачите со безбедносните стандарди мора редовно да се следи преку ревизии, безбедносни прашалници и стрес тестови.
- Споделување информации: Субјектите треба да промовираат отворено пријавување на безбедносни инциденти од добавувачи и да споделуваат релевантни разузнавачки информации за закани за да избегнат познати напади.
- Ревизии: За добавувачите со висок ризик, треба редовно да се спроведуваат безбедносни ревизии и да се прегледува нивната безбедносна состојба.
- Соработка при одговор на инциденти: Субјектите мора да бидат подготвени да обезбедат поддршка на добавувачите за време на безбедносен инцидент ако тоа може да влијае на работните процеси или поширокиот ланец на снабдување.
- Процедури за раскинување: Мора да се воспостават формални процедури за безбедно повторно враќање на контролата од страна на субјектите во однос на нивните средства и одземање на пристапот од добавувачите на крајот од договорот.

Безбедност при набавка, развој и одржување на мрежни и информациски системи

Член 6

Петтиот чекор за управување со ризиците кои претставуваат закана за мрежните и информациските системи е безбедност при набавка, развој и одржување на мрежни и информациски системи.

Овој чекор ги опфаќа барањата за обезбедување дека целата технологија од софтвер и хардвер до цели системи е изградена, стекната и одржувана, со безбедноста како централна грижа од самиот почеток и опфаќа:

- Безбеден дизајн: Субјектите се должни да ги интегрираат безбедносните барања и да ги моделираат на закани во почетните фази на планирање и дизајн на секој нов систем или развој на апликација. Ова вклучува користење на безбедни дизајнерски шеми и спроведување безбедносна ревизија на дизајнот.
- Безбедно кодирање: Субјектите се должни да ги следат безбедните практики за кодирање, да користат статички и динамички алатки за анализа и да спроведуваат редовни прегледи на кодот за да ги идентификувааат и отстранат ранливостите за време на развојниот процес.
- Управување со ранливости: Субјектите се должни да воспостават формална, документирана политика за управување со ранливости за систематско идентификување, евалуација и адресирање на безбедносните слабости. Оваа политика треба да ги дефинира процесите и временските рамки за санација.
- Редовно скенирање на ранливости: Субјектите се должни редовно да ги скенираат ранливостите на сите мрежни системи и апликации за идентификување на слабости и погрешни конфигурации.
- Управување со закрпи: Субјектите се должни да имплементираат робустен систем за управување со безбедносни ажурирања за брзо применување и ажурирање на целиот хардвер, софтвер и системи. Политиката за управување со ранливости треба да ги специфицира процесите за ова.
- Безбедно распоредување: Субјектите се должни да ги следат практиките за безбедно распоредување, вклучувајќи спроведување безбедносни проценки на средината за распоредување и имплементација на соодветни безбедносни контроли.
- Сертифицирани производи: Субјектите се должни да користат ИКТ услуги, системи и производи кои се сертифицирани врз основа на европски и меѓународни шеми за сертификација за сајбер безбедност каде што таквите шеми се применливи и достапни.
- Безбедно одржување: Субјектите се должни континуирано да даваат приоритет на безбедноста во фазата на одржување преку следење на нови ранливости, ажурирање на системи и редовни безбедносни прегледи за да се осигураат дека системот останува безбеден со текот на времето.
- Интеграција на разузнавачки информации за закани: Субјектите се должни да користат разузнавачки информации за закани за да идентификуваат трендови и шеми кои можат да укажат на идни безбедносни пропусти. Овие информации треба да се користат за да се приоритизираат напорите за закрпување и санација.
- Редовен преглед и одобрување: Субјектите се должни сите политики поврзани со набавка, развој и одржување редовно да ги прегледуваат и

ажурираат за да се адресираат новите закани и промени во ИТ средината. Овие политики формално се одобруваат од раководството на институцијата.

Политики и процедури за проценка на ефикасноста

Член 7

Шестиот чекор за управување со ризиците кои претставуваат закана за мрежните и информациските системи е воспоставување на политики и процедури за проценка на ефикасноста.

Политиките и процедурите за проценка на ефикасноста вклучуваат:

- Усвојување на рамка: Субјектите се должни безбедносните практики да ги усогласат со призната рамка како NIST Cybersecurity Framework, ISO/IEC 27001 или CIS Controls, што обезбедува систематски, ревидиран пристап кон управувањето со ризици.
- Документација за политики и процедури: Потребно е субјектите да создадат јасни, лесни за читање и редовно ажурирани политики и процедури за сајбер безбедност. Оваа документација треба да ги опише безбедносните очекувања и улоги за сите вработени. Сите релевантни документи мора да бидат одобрени од високото раководство.
- Годишни безбедносни ревизии: Субјектите треба да спроведуваат формални, независни безбедносни ревизии најмалку еднаш годишно за да се споредат политиките за сајбер безбедност на организацијата со нејзините реални практики. Ревизијата мора да ја утврди изложеноста на организацијата на внатрешни и надворешни закани.
- Таргетирани ревизии: Субјектите мора да бидат подготвени да спроведуваат таргетирани безбедносни ревизии извршени од независен ревизор за сајбер безбедност кога ќе го побара надлежниот орган, како што е уредено со Законот за безбедност на мрежни и информациски системи.
- Континуирано следење: Субјектите мора да имплементираат систем за управување со безбедносни информации и настани (SIEM) или слични алатки за континуирано следење на мрежната активност и однесувањето на корисниците за откривање на аномалии и безбедносни настани во реално време.
- Логирање на инциденти и настани: Субјектите се должни сите безбедносни инциденти и системски настани правилно да ги евидентираат и евиденцијата да ја чуваат за утврден временски период за форензичка анализа и ревизија.
- Следење на отстранување: Субјектите мора да имплементираат систем за следење на сите идентификувани ранливости и погрешни конфигурации за да се осигура дека тие се правилно адресирани.
- Ревизија и преглед на политики: Субјектите се должни периодично да ги ревидираат политиките и процедурите за сајбер безбедност за да се осигураат дека тие сè уште се релевантни и ефективни. Овој процес треба да ги вклучи клучните засегнати страни и да се справи со низа внатрешни и надворешни закани.

- Анализа на ризик: Субјектите се должни редовно да ја преоценуваат толеранцијата на ризик и потенцијалното влијание од безбедносните инциденти врз континуитетот на нивното работење и обезбедувањето на јавни услуги. Ова придонесува за усогласување на распределбата на ресурсите за безбедносни контроли со целите и надлежностите на институцијата.
- **Надворешни скенирања**: Субјектите се должни да спроведуваат проактивно, неинтрузивно скенирање на јавно достапни мрежни и информациски системи за идентификување на ранливи или лошо конфигурирани системи.

Основна сајбер хигиена и обука за сајбер безбедност

Член 8

Шестиот чекор за управување со ризиците кои претставуваат закана за мрежните и информациските системи е воспоставување на основна сајбер хигиена и обука за сајбер безбедност, која опфаќа:

- Задолжителна програма за обука: Министерството за дигитална трансформација е должно да спроведува задолжителна, континуирана програма за обука за сајбер безбедност за сите вработени, соработници, назначени сајбер офицери од страна на конституентите како и друг релевантен кадар и засегнати страни.
- Теми за обука: Обуката треба да опфати низа критични теми, вклучувајќи како да се препознаат фишинг напади, социјално инженерство, малициозен софтвер и правилно управување со лозинки. Треба да вклучува и обука за безбедна употреба на преносливи уреди, физички пристап, уништување на податоци и енкрипција.
- Политика за силна лозинка: Субјектите се должни да спроведат политика за силна лозинка која налага комплексност, забранува повторна употреба и бара редовна ротација на лозинки за сите сметки.
- Заштита од фишинг: Субјектите се должни да имплементираат и обезбедат обука за користење на алатки и процедури против фишинг, бидејќи фишинг и шемите за социјално инженерство претставуваат распространет метод кој го користат сајбер криминалците и претставуваат чести закани за сајбер безбедноста.
- Политика за користење на уреди: Субјектите се должни да креираат јасни, документирани политики за користење на лични уреди за работа и користење на службени уреди за лични активности за спречување на необезбедени влезни точки.
- Редовни ажурирања и закрпи: Субјектите се должни да обезбедат редовно ажурирање на целиот софтвер, вклучувајќи ги оперативните системи и апликациите, како и навремена примена на безбедносните закрпи.
- Обука за пријавување инциденти: Субјектите се должни да ги обучат сите вработени како веднаш да идентификуваат и пријават сомнителни активности или потенцијални безбедносни инциденти до надлежните лица.
- Политики за контрола на пристап: Субјектите се должни да ги обучат

вработените за принципот на најмала привилегија и други политики за контрола на пристап за да се спречи неовластен пристап до чувствителни податоци и системи.

- Воведување/Отпуштање на вработени: Субјектите се должни да ја интегрираат свесноста за сајбер безбедност во процесот на вклучување на вработените при засновање на работен однос како и да осигураат дека безбедноста е приоритет при престанок на работниот однос, вклучувајќи навремено одземање на правата на пристап.
- Редовен преглед и одобрување: Политиките и програмите за обука се прегледуваат најмалку еднаш годишно, со цел да се обезбеди нивна релевантност и ефективност. Сите промени во овие политики мора да бидат документирани и одобрени од претставникот или високото раководство на субјектот.

Употреба на криптографски техники и енкрипција

Член 9

Седмиот чекор за управување со ризиците кои претставуваат закана за мрежните и информациските системи е употреба на криптографски техники и енкрипција за заштита на чувствителните податоци од неовластен пристап или модификација, како кога податоците се чуваат така и кога се пренесуваат.

Употреба на криптографски техники и енкрипција вклучува:

- Класификација на податоци: Податоците мора да се класифицираат според нивото на чувствителност со цел да се примени соодветна енкрипција врз основа на критичноста и класификацијата на податоците.
- Енкрипција на податоци во мирување: Целосната енкрипција на дискот мора да се користи за сите уреди и медиуми кои чуваат чувствителни или класифицирани податоци за заштита од неовластен физички пристап.
- Енкрипција на податоци во транзит: Податоците пренесени преку јавни мрежи мора да бидат шифрирани со безбедни протоколи како Transport Layer Security (TLS 1.3), IPsec или S/MIME за да се обезбеди доверливост и интегритет.
- Политика за управување со клучеви: Мора да се имплементира формална политика за управување со клучеви, која го опфаќа целиот животен циклус на криптографските клучеви, од безбедно генерирање и дистрибуција до складирање, ротација и уништување. Оваа политика мора формално да биде одобрена од високото раководство и редовно да се прегледува.
- Употреба на силни алгоритми: Субјектите се должни да обезбедат употреба на модерни, одобрени алгоритми како AES-256 за симетрична енкрипција и RSA со минимална должина на клучот од 2048 бита за асиметрична енкрипција. Застарени алгоритми како DES или RC4 се забранети.
- Безбедно складирање на клучеви: Криптографските клучеви мора да се чуваат безбедно, одделени од кодот на апликацијата. За оваа намена потребно е да се користат хардверски безбедносни модули (HSM) или услуги за управување со клучеви базирани во облак (KMS).

- Ротација на клучот: Мора да се имплементира распоред за периодична ротација на клучеви за да се минимизира влијанието на компромитиран клуч. Клучевите мора веднаш да се ротираат ако се сомнева на пробив.
- Енкрипција од крај до крај: Каде што е можно, потребно е да се имплементира енкрипција од крај до крај за да се осигура дека податоците се шифрирани на изворот и ќе се дешифрираат само на нивната крајна дестинација, спречувајќи посредници да пристапат до нив при нивниот пренос.
- Враќање на клучеви: Криптографската опрема и апликации мора да обезбедат средство за враќање на податоци во случај да се изгуби, оштети или откаже клуч за енкрипција.
- Логирање и ревизија: Сите активности поврзани со клучеви мора да се евидентираат за ревизија, а треба да се имплементираат контроли на пристап за да се осигура дека само овластени лица или системи можат да ракуваат со чувствителни клучеви.

Безбедност на човечките ресурси, политики за контрола на пристап и управување со средства

Член 10

Седмиот чекор за управување со ризиците кои претставуваат закана за мрежните и информациските системи е безбедност на човечките ресурси, политики за контрола на пристап и управување со средства.

Овој чекор ги адресира критичните организациски мерки потребни за управување со внатрешниот ризик, заштита на средствата и контрола на пристапот до системи и податоци и се фокусира на политиките што го регулираат пристапот на вработените низ целиот нивен животен циклус и на сеопфатното следење на сите ИТ средства и опфаќа:

- Политика за животен циклус на безбедност на човечки ресурси: Мора да се спроведе сеопфатна политика за сајбер безбедност на човечки ресурси која ги адресира безбедносните барања пред, за време и по завршувањето на работниот однос. Оваа политика мора формално да биде одобрена од раководното лице на субјектот.
- Безбедносни проверки: Безбедносните проверки мора да се спроведат за сите лица кои ќе имаат привилегиран пристап до критични системи и чувствителни податоци.
- Улоги и одговорности: Улогите и одговорностите во сајбер безбедноста мора јасно да бидат дефинирани во описите на работните места. Вработените мора да ги разберат и да се согласат со своите обврски за сајбер безбедност.
- Политика за контрола на пристап: Мора да се спроведе принцип на најмала привилегија (PoLP), кој обезбедува корисниците да имаат само минимален пристап потребен за извршување на своите работни функции. Оваа политика мора формално да биде одобрена од раководното лице на субјектот и редовно прегледувана.
- Одземање на пристап: Субјектот потребно е да спроведе процедури за

неодложно одземање на сите права на пристап до мрежата и системот по престанок на работниот однос или промена на улогата на вработениот.

- Сеопфатен попис на средства: Потребно е да се создаде и одржува детален, ажуриран попис на сите ИТ средства, вклучувајќи хардвер, софтвер, претплати во облак и договори со добавувачи. Треба да се користат повеќе методи за откривање за да се обезбеди точност.
- Класификација на средства: Сите средства неопходно е да се класифицираат врз основа на нивната критичност, вредност и чувствителност за да се даде приоритет на управувањето и безбедносните напори.
- Управување со животниот циклус на средствата: Субјектите се должни да имплементираат систем за следење на средствата низ целиот нивен животен циклус, од набавка до отстранување, за да се осигура дека остануваат безбедни и евидентирани.
- Редовни ревизии на пристап: Субјектите се должни да спроведуваат редовни ревизии на кориснички сметки и права на пристап за да се идентификуваат и отстранат застарени или непотребни привилегии.
- Безбедно отстранување: Мора да се следат безбедни и еколошки одговорни процедури за отстранување на средства, вклучувајќи отстранување на сите податоци од хардверот.

Користење на мултифакторска автентифкација (MFA) и безбедни комуникациски системи

Член 11

Седмиот чекор за управување со ризиците кои претставуваат закана за мрежните и информациските системи е користење на мултифакторска автентифкација (во натамошниот текст: МФА) и безбедни комуникациски системи.

Овој чекор ги опфаќа двете критични мерки за заштита од неовластен пристап и обезбедување на интегритетот и доверливоста на комуникациските канали и содржи:

- МФА за привилегирани сметки: Користењето на мултифакторска автентифкација мора да биде задолжително за сите привилегирани или административни сметки. Ова е најкритичниот прв чекор во МФА политиката.
- МФА за далечински пристап: МФА мора да биде задолжителен за сите конекции за далечински пристап, вклучувајќи VPN и услуги за далечински десктоп, бидејќи тие се точки со висок ризик.
- МФА за е-пошта и услуги во облак: МФА треба да се спроведува за пристап до службена е-пошта, услуги во облак и системи за складирање датотеки.
- Користење на МФА отпорни на фишинг: Субјектите треба да имплементираат и поттикнат употреба на побезбедни, "фишинг-отпорни" МФА методи како FIDO безбедносни клучеви или паметни картички, кои се сметаат за златен стандард.
- Адаптивна автентифкација: Решенијата за адаптивна автентифкација треба да се имплементираат за динамично зголемување или намалување на чекорите за автентификација на корисникот врз основа на контекстуални информации

како локација, уред или време од денот.

- Безбеден глас, видео и текст: Внатрешната гласовна, видео и текстуална комуникација мора да биде заштитена со соодветна енкрипција за да се спречи пресретнување и прислушување.
- Безбедна итна комуникација: Мора да се воспостави и одржува безбеден систем за итна комуникација кој не се потпира на јавни мрежи. Ова може да вклучува VHF/UHF радио, сателитски телефони или други посветени канали за користење во случај на дефект на мрежата.
- Политика за внатрешна комуникација: Мора да се развие формална политика која прецизира кои комуникациски канали се одобрени за различни типови информации врз основа на нивната чувствителност. Оваа политика мора формално да биде одобрена од високото раководство на субјектот.
- Обука на вработените: Сите вработени мора да бидат едуцирани за важноста на МФА и правилната употреба на безбедни комуникациски системи за да се обезбеди прифаќање и усогласеност од страна на корисниците.
- Континуирано следење: Сите логови за автентификација и комуникација мора континуирано да се следат за да се откријат сомнителни активности и потенцијални компромитирања.

Насоки за имплементација и усогласеност

Член 12

Во табелата е даден преглед на техничките и методолошките барања за мерки за управување со ризиците кои претставуваат закана за мрежните и информациските системи во Владата, министерствата, самостојните органи на државната управа, органите на државната управа во состав на министерствата, управните организации, општините, општините во градот Скопје и градот Скопје. Со „З“ се означени задолжителните барања, а со „П“ се означени препорачаните барања.

Чекор	Барање	Опис	Суштински субјект	Важен субјект
Анализа на ризиците за безбедност на мрежните и информациските системи	1.1. Дефинирање на обем и цели	Дефинирајте го обемот и целите на проценката на ризикот, идентификувајќи кои системи, мрежи и работни процеси се вклучени во анализата, во согласност со работните цели.	З	П

	1.2. Идентификација и класификација на средства	Креирајте и одржувајте сеопфатен попис на сите критични ИТ средства, класифицирајќи ги според вредност и критичност за работните процеси.	З	З
	1.3. Идентификација на закани и ранливости	Активно идентификувајте потенцијални внатрешни и надворешни закани и ранливости користејќи рамки како MITRE ATT &CK.	З	З
	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 за квантитативна проценка базиран на податоци.	З	З
	1.5. План за справување со ризик	Развијте и документирајте конкретен, остварлив план за справување со ризици со висок приоритет, со утврдени одговорни страни, временска рамка и индикатори и	З	П

		критериуми за следење на реализација на препораките.		
	1.6. Имплементација на безбедносна контрола	Воведете и превентивни и тековни контроли за намалување на идентификуваните ризици.	З	З
	1.7. Континуирано следење	Воспоставете процес за континуирано следење на безбедносната состојба, вклучувајќи редовни скенирања на ранливости и тестирања на пенетрација.	З	П
	1.8. Редовен преглед и одобрување	Спроведувајте и одобрувајте проценки на ризик најмалку еднаш годишно и по значајни промени во ИТ средината.	З	З
	1.9. Комуникација со засегнатите страни	Комуницирајте ги резултатите од проценката и плановите за справување со високото раководство и клучните засегнати страни, прилагодувајќи ги извештаите на лицата на кои се однесуваат.	З	З

	1.10. Документирање	Документирајте го целиот процес на проценка на ризикот, вклучувајќи методологии, идентификувани ризици и имплементирани контроли.	3	3
Управување 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 вообичаените, 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 инциденти (задолжително)	Веднаш, и најдоцна три часа по дознавањето, известете го	3	3

		надлежнниот CSIRT за било каков значаен инцидент или закана.		
	2.5. Навремено известување и конечен извештај	Да се обезбеди рано предупредување во рок од 24 часа од дознавање за значаен инцидент и детален извештај во рок од 72 часа. Конечниот извештај мора да биде доставен во рок од еден месец од решавањето на инцидентот.	3	3
	2.6. Спречување	Спроведете краткорочни и долгорочни мерки за спречување на ширењето на инцидентот, како што е изолирање на погодените системи.	3	3
	2.7. Отстранување	Целосно отстранете ја заканата од сите погодени системи. Ова вклучува отстранување на малициозен софтвер и поправка на ранливости и ресетирање на компромитирани кредендијали.	3	3
	2.8. Опоравување	Вратете ги засегнатите системи во нормална работа	3	3

		користејќи тестирани резервни копии.		
	2.9. Преглед по инцидентот	Спроведете формален преглед по инцидентот за да го утврдите изворот на причината, идентификувајќи ги позитивните аспекти при справување со инцидентот и документирајте ги научените лекции.	З	З
	2.10. Прирачници и вежби	Развивајте и одржувајте прирачници за одговор на инциденти за вообичаени закани и спроведувајте практични вежби.	З	П
Континуитет на работењето, обновување по катастрофи и управување со кризи	3.1. Анализа на влијанието врз работните процеси (BIA)	Спроведете BIA за да ги идентификувате и приоритизирате основните работни функции и нивните поддржувачки ИТ системи.	З	З
	3.2. Цели за опоравување	Воспоставете јасни Цели за време на опоравување (RTOs) и Цели на точки за опоравување (RPO) за секој критичен ресурс.	З	З

	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.	З	З
	3.4. План за обновување од 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 работните процеси.	З	П
	3.7. Комуникациски план	Осигурајте се дека комуникацискиот план вклучува протоколи за	З	З

		користење безбедни, алтернативни канали во случај на дефект на мрежата.		
	3.8. Попис на средства	Одржувајте детален попис 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 работните процеси и обновување по катастрофи.	З	П
Безбедност на ланецот на снабдување	4.1. Управување и одобрување	Назначете одговорно лице за безбедност на ланецот на снабдување и имајте формална политика одобрена од	З	П

		високото раководство.		
	4.2. Регистар на ризици	Осигурајте се дека ризиците во ланецот на снабдување формално се евидентирани во регистарот на ризици на субјектот 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 поедноставите надзорот на ризикот.	З	П
	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 прашалници и стрес тестови.	З	П
	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 раскинување	Воспоставете формални процедури за безбедно повторно враќање на контролата врз вашите средства и	З	З

		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 идентификување, евалуација и адресирање на безбедносните слабости.	3	3
	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.	З	З
	5.6. Безбедно распоредување	Следете ги практиките за безбедно распоредување, вклучувајќи спроведување безбедносни проценки на средината за распоредување.	З	З
	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	З	П

		укажуваат на идно безбедносно прекршување.		
	5.10. Редовен преглед и одобрување	Редовно прегледувајте и ажурирајте политики поврзани со набавка, развој и одржување, со формално одобрување од високото раководство.	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 високото раководство.	З	З
	6.3. Годишни безбедносни ревизии	Спроведете формални, независни безбедносни ревизии најмалку еднаш годишно за споредба на политиките за сајбер безбедност на организацијата со нејзините реални практики.	З	П

	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 и одржувани во одреден период за форензичка анализа.	З	З
	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	З	О

		релевантни и ефективни.		
	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.	3	0
	6.10. Надворешни скенирања	Спроведете проактивно, неинвазивно скенирање на јавно достапни мрежни и информациски системи за идентификување на ранливости.	3	0
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.	3	3
	7.2. Теми за обука	Обуката треба да опфати фишинг, социјално инженерство, малициозен софтвер, управување со лозинки и безбедна употреба на преносливи уреди.	3	3

	7.3. Политика за силна лозинка	Спроведете политика за силна лозинка која налага комплексност, забранува повторна употреба и бара редовна ротација на лозинки.	3	3
	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	3	3

		безбедносни инциденти.		
	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. Вработување/Отстранување на вработени	Интегрирајте ја свесноста за сајбер безбедност при засновањето на секој работен однос и обезбедете 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 еднаш годишно.	3	3
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	3	3

		чувствителни или класифицирани податоци.		
	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.	З	З
	8.4. Политика за управување со клучеви	Имплементирајте формална, одобрена политика за управување со клучеви која го опфаќа целиот животен циклус на криптографските клучеви.	З	З
	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	З	З

		периодична ротација на клучот за да го минимизирате влијанието на компромитиран клуч.		
	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 оправување 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 на работното место, со формално одобрување од високото раководство.	З	З

	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 пристап потребен за нивните работни функции.	З	З
	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.	З	З

	9.6. Сеопфатен инвентар на средства	Креирајте и одржувајте детална, ажурирана инвентар на сите ИТ средства користејќи повеќе методи за откривање за точност.	З	З
	9.7. Класификација на средства	Класифицирајте ги сите средства врз основа на нивната бизнис критичност, вредност и чувствителност за да ги приоритизирате управувачките и безбедносните напори.	З	З
	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	З	З

		средства, вклучувајќи отстранување на сите податоци од хардверот.		
Употреба на мултифакторска автентификација (MFA) и безбедни комуникациски системи	10.1. MFA за привилегирани сметки	Задолжително користење на мултифакторска автентификација 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 услуги во облак	Спроведете MFA за пристап до службена е-пошта, услуги во облак и системи за складирање датотеки.	З	П
	10.4. Користење на MFA отпорен на фишинг	Имплементирајте и поттикнете употреба на MFA методи отпорна на фишинг, како што се FIDO безбедносни клучеви или паметни картички.	З	П
	10.5. Адаптивна автентификација	Имплементирајте адаптивни решенија за автентификација кои динамично ги	З	П

		зголемуваат или намалуваат чекорите за автентификација врз основа на контекстуални информации.		
	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 одобрени за различни типови информации.	З	З
	10.9. Обука на вработени	Едуцирајте ги сите вработени за важноста на MFA и правилната употреба на безбедни комуникациски системи.	З	З

	10.10. Континуирано следење	Континуирано следете ги сите логови за автентификација и комуникација за да откриете сомнителни активности и потенцијални компромитирања.	3	3

Резиме на нивоа на барања
Член 13

Разликата помеѓу нивоата на барањата за суштинските и важните субјекти е следна:

Чекор	**Суштинска субјект**	**Важен субјект**
1. Анализа на ризик	Целосна имплементација на сите барања, со редовни, формални ревизии.	Задолжителни основни барања; Поголема флексибилност во континуирано следење и специфични контроли.
2. Справување со инциденти	Задолжително, брзо и сеопфатно известување. Потребни се вежби и посветен офицер за сајбер безбедност.	Задолжително, брзо и сеопфатно известување, со препораки за вежби и посветени улоги на одговорните лица.
3. Континуитет на работните процеси	Задолжително, редовно тестирање на планови со фокус на сеопфатно закрепнување на критичните функции.	Задолжителни, документирани планови со препораки за редовно тестирање и управување со кризи.
4. Безбедност на ланецот на снабдување	Задолжителна длабинска проверка, договорни клаузули и континуирано следење за сите добавувачи.	Задолжителни основни договорни клаузули со препораки за поширока длабинска проверка и мониторинг.
5. Набавка/развој	Задолжително безбедно управување со животниот циклус и набавка на сертифицирани производи каде што е достапно.	Задолжително безбедно управување со животниот циклус со препораки за сертификација на производот.

6. Проценка на ефикасноста	Задолжително усогласување со безбедносна рамка, редовни ревизии и континуирано следење.	Препорачано усогласување со рамка, со задолжителна документација на политики и процедури.
7. Хигиена и обука	Задолжителна, сеопфатна и континуирана обука за сите вработени.	Задолжителна, сеопфатна и континуирана обука за сите вработени.
8. Криптографија	Задолжителна употреба на силни стандарди за енкрипција и целосна политика за управување со клучеви.	Задолжителна употреба на силни стандарди за енкрипција со препораки за напредно управување со клучеви.
9. ЧР безбедност/контрола на пристап	Задолжително целосно управување со вработените лица, контроли на пристап и сеопфатен попис на средства.	Задолжително управување со цел животен циклус на вработените лица и контроли на пристап.
10. МФА/Безбедни комуникации	Задолжителна МФА за сите привилегирани и далечински пристапи, како и безбеден систем за итна комуникација.	Задолжителна МФА за привилегиран и далечински пристап со препораки за безбеден систем за итна комуникација.

Влегување во сила
Член 14

Овој правилник влегува во сила наредниот ден од денот на објавувањето на веб страната на Министерството за дигитална трансформација.

Бр. 10-13441
03.06 година 2026
Скопје

Министер за дигитална трансформација,
Стефан Андоновски