РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
REPUBLIKA E MAQEDONISË SË VERIUT
МИНИСТЕРСТВО ЗА ОДБРАНА
MINISTRIA E MBROJTJES
Бр.-Nr. 01 - 2841/1
14 -09- 2026 20
Скопје-Shkup

Република Северна Македонија

Министерство за одбрана

ПРАВИЛНИК

ЗА КОРИСТЕЊЕ НА ИНФОРМАТИЧКО КОМУНИКАЦИСКИТЕ ТЕХНОЛОГИИ ВО МИНИСТЕРСТВО ЗА ОДБРАНА

Август 2026 година

СОДРЖИНА

1. Намена. 3
2. Делокруг. 4
3. Одговорности 4
4. Основни принципи на Правилникот 5
4.1. Користење на информатичките системи на Министерството за одбрана 6
4.2. Користење на интернет **Error! Bookmark not defined.**
4.3. Користење на службената електронска пошта 7
4.3.1 Пристап до службената електронска пошта од надворешни и приватни уреди 8
4.4. Лозинки и автентикација 8
4.5. Користење на мобилни уреди 9
4.6. Користење на надворешни медиуми 10
4.7. Користење на услуги во облак 10
4.8. Користење на генеративна вештачка интелигенција (AI) 10
4.9. Користење на социјални мрежи 11
5. Мониторинг на информатичките системи и средства 12
6. Пријавување безбедносни инциденти 12
7. Непочитување на Правилник 12
8. Завршни одредби 13

Врз основа на член 55 став (1) од Законот за организација и работа на органите на државната управа („Службен весник на Република Македонија“ бр. 58/00, 44/02, 82/08, 167/10, 51/11 и „Службен весник на Република Северна Македонија“ бр. 96/19 и 110/19), а во врска со член 20 точки 26) и 30) од Законот за одбрана („Службен весник на Република Македонија“ бр. 42/01, 5/03, 58/06, 110/08, 51/11, 151/11, 215/15 и „Службен весник на Република Северна Македонија“ бр. 42/20), министерот за одбрана, донесе

ПРАВИЛНИК

ЗА КОРИСТЕЊЕ НА ИНФОРМАТИЧКО КОМУНИКАЦИСКИТЕ ТЕХНОЛОГИИ ВО МИНИСТЕРСТВО ЗА ОДБРАНА

I.ОПШТИ ОДРЕДБИ

Член 1

Со овој правилник се утврдува намената за користење на Информатичко Комуникациските Технологии (во натамошниот текст: ИКТ) во Министерството за одбрана (во натамошниот текст: Министерството), делокругот на користење, одговорностите, основните принципи за користење на ИКТ, мониторингот на информатичките системи и средства, пријавување на безбедносните инциденти и непочитување на одредбите на правилникот.

II.НАМЕНА ЗА КОРИСТЕЊЕ

Член 2

Правилникот за прифатливо користење на ИКТ во Министерството, воспоставува јасни правила, одговорности и прифатливо однесување за сите корисници кои пристапуваат до информатичките системи, мрежи и дигитални ресурси на Министерството. Со имплементацијата на овој Правилник ќе се зајакнува севкупната сајбер отпорност на Министерството, со тоа што им овозможува на корисниците да ги разберат своите улоги во заштитата на информации, одржувањето на безбедноста на мрежата и спречувањето на неовластени активности. Правилникот обезбедува усогласеност и почитување на националните регулативи, стандардите на НАТО, ЕУ и меѓународните рамки за сајбер безбедност. Исто така опфаќа и препораки кои се добиени од интерни контроли на мрежната инфраструкрура на Министерството. Со поставување на јасни очекувања и овозможување на одговорност преку следење и спроведување, Правилникот го штити оперативниот интегритет, ги ублажува сајбер ризиците и го

промовира одговорното користење на ИКТ, мрежите и информатичките системи на Министерството.

III.ДЕЛОКРУГ НА КОРИСТЕЊЕ

Член 3

Овој Правилник се однесува на сите вработени, раководни лица, надворешни соработници, консултанти, лица ангажирани по договор, лица на пракса, слушатели на Воената академија и сите други лица кои поседуваат одобрена корисничка сметка или пристапни акредитиви - овластен пристап до компјутерските системи и мрежи на Министерството. Правилникот ги опфаќа сите активности што се спроведуваат преку користење на уредите: десктоп и лаптоп компјутери, сервери, мобилни телефони, таблет уреди, виртуелни работни станици и околини и сите други ИКТ средства и услугите: електронска пошта, интернет услуги, безжични мрежи, услуги во облак, службени апликации, како и комуникациски услуги во сопственост или управувани од Министерството. Усогласеноста со Правилникот обезбедува придржување кон воспоставените безбедносни, оперативни и етички стандарди што го регулираат користењето на системите и податоците на Министерството.

IV.ОДГОВОРНОСТИ

Член 4

Министерот за одбрана, со донесувањето на овој Правилник го определува Директоратот за комуникации /Секторот К4 – ИКТ, како одговорен носител за планирање, организирање, спроведување и следење на примената на овој Правилник.

Директоратот за комуникации/Секторот К4 – ИКТ обезбедува континуирана информатичка поддршка, воспоставување и одржување на соодветни технички и организациски мерки за заштита на информатичките системи, дигиталните податоци и конфигурациските поставки, како и спроведување на контроли за зачувување на доверливоста, интегритетот и расположливоста на информациите.

Примената на овој Правилник се обезбедува преку воспоставување и спроведување на технички контроли, административни процедури, едукација на корисниците, како и редовни проверки и ревизии на усогласеноста со одредбите од овој Правилник.

Секој корисник на информатичките системи и сервиси на Министерството е должен да ги почитува одредбите на овој Правилник, да ги заштитува службените информации во сопственост на Министерството и информатичките средства што му се доверени на користење и без одлагање да ги пријавува сите безбедносни инциденти, сомневања за злоупотреба и други неправилности во согласност со утврдените процедури.

Запознавањето со одредбите на овој Правилник и обврската за нивно почитување се потврдува со потпишување на Изјава за прифаќање на правилата за користење на информатичките средства и системи.

V.ОСНОВНИ ПРИНЦИПИ НА ПРАВИЛНИКОТ ЗА КОРИСТЕЊЕ НА ИКТ ВО МИНИСТЕРСТВОТО

Член 5

Информатичките средства, системи, мрежната инфраструктура и дигиталните услуги, претставуваат средства во сопственост на Министерството и се наменети за извршување на службените задачи. На корисниците им се доделуваат на користење согласно нивните работни обврски и службени овластувања.

Сите средства во сопственост на Министерството задолжително се означуваат со трајна и видлива ознака за сопственост, која содржи податоци за припадноста на средството, инвентарен број и други идентификациски податоци утврдени со интерните акти.

Заради заштита од неовластено отворање или манипулација, средствата се обезбедуваат со заштитни безбедносни налепници или други соодветни механизми за заштита, поставени на начин што овозможува евидентирање на секој обид за нивно неовластено отворање или измена.

Секој корисник е лично одговорен за сите активности што се извршуваат преку неговата корисничка сметка, без оглед на средството преку кое пристапува до информатичките системи и сервисите на Министерството.

Корисникот е должен доделените информатички средства да ги користи правилно, безбедно, наменски и во согласност со нивната функција, како и да ги заштитува од губење, оштетување, злоупотреба и неовластено користење.

Корисникот не смее да го отстапува на користење доделеното информатичко средство на друго лице, без претходно одобрение од овластено лице во Министерството.

Пристапот до информатичките системи на Министерството преку приватни уреди е дозволен, само доколку таквиот пристап е одобрен и уредот ги исполнува безбедносните барања утврдени од Министерството.

Сите корисници се должни да постапуваат во согласност со важечките закони, подзаконските акти, интерните политики, безбедносните процедури и другите акти со кои се уредува информациската безбедност во Министерството.

5.1.Користење на ИКТ, информатичките средства, системите и сервисите на Министерството

Член 6

ИКТ, информатичките средства, системите и сервисите на Министерството се користат за извршување на службените задачи и работните обврски на корисниците.

Користењето на ИКТ, информатичките средства, системите и сервисите на Министерството е дозволено за службена комуникација, пристап до службените информатички системи, обработка и размена на службени информации, стручно усовршување поврзано со работното место, како и за ограничено лично користење, доколку тоа не влијае врз безбедноста, расположливоста, интегритетот на информатичките системи или врз извршувањето на службените задачи.

На информатичките средства и системи на Министерството, е забрането:

- инсталирање, користење или отстранување софтвер без претходно одобрение од надлежната организациска единица овластена од Директоратот за комуникации;
- користење неовластен, нелиценциран или пиратски софтвер;
- заобиколување, оневозможување или нарушување на воспоставените безбедносни механизми и контроли;
- менување на системските поставки, конфигурации и безбедносни параметри без овластување;
- користење корисничка сметка што му припаѓа на друго лице;
- откривање, споделување или отстапување лозинки, токени, сертификати или други средства за автентикација;
- поврзување на неовластени жични, безжични, информатички и други комуникациски уреди, како и воспоставување неовластени безжични пристапни точки (Wi-Fi hotspot) на мрежата на Министерството;
- користење приватни USB-уреди или други преносни мемориски медиуми без претходно одобрение;
- преземање, складирање или дистрибуција на нелегална, злонамерна или несоодветна содржина;
- користење на информатичките средства за приватна стопанска дејност, политички активности или стекнување лична материјална корист и
- преземање активности што можат да ја загрозат доверливоста, интегритетот, расположливоста или угледот на Министерството;

Корисниците се должни, при секое привремено отсуство од работното место, да ги заклучуваат уредите што ги користат, со цел да се спречи неовластен пристап до информациите и информатичките системи.

Секое користење на информатичките средства и системи спротивно на одредбите од овој Правилник претставува неовластено користење и подлежи на постапување согласно важечките законски прописи и интерните акти на Министерството.

5.2.Користење на интернет

Член 7

При користење на интернет, корисниците се должни да постапуваат совесно и одговорно и да го користат интернет-пристапот исклучиво за службени потреби или за ограничено лично користење што не влијае врз безбедноста и непреченото функционирање на информатичките системи.

Корисниците се должни:

- да пристапуваат само до веб-страници што се поврзани со извршувањето на службените задачи или не претставуваат безбедносен ризик;
- да преземаат датотеки исклучиво од доверливи и проверени извори;
- да не посетуваат веб-страници што содржат злонамерна, незаконска, навредлива или друга несоодветна содржина;
- да не користат VPN, прокси-сервери, услуги за прикривање на идентитетот и локацијата или други механизми за заобиколување на безбедносните контроли без претходно одобрение и
- да не преземаат активности што можат да доведат до компромитирање на информатичките системи или мрежната инфраструктура на Министерството.

5.3.Користење на службената електронска пошта

Член 8

Службената електронска пошта се користи исклучиво за службени комуникации и размена на информации поврзани со извршувањето на работните задачи.

При користење на службената електронска пошта, корисниците се должни:

- внимателно да ја проверуваат автентичноста на испраќачот и содржината на електронските пораки;

- да не отвораат сомнителни пораки, прилози или интернет-врски;
- да не доставуваат доверливи или класифицирани информации на неовластени лица;
- да не овозможуваат автоматско препраќање на службената електронска пошта кон приватни сметки за е-пошта без претходно одобрение;
- без одлагање да пријават сомнителни пораки, обиди за фишинг, малициозен софтвер или други облици на злоупотреба и
- да не ја користат службената електронска пошта за регистрација, креирање кориснички сметки, најава или користење на приватни веб-портали, интернет-услуги, апликации и други онлајн сервиси кои не се поврзани со извршувањето на службените задачи.

5.3.1. Пристап до службената електронска пошта од надворешни и приватни уреди

Член 9

Пристапот до службената електронска пошта од надвор од информациско-комуникациската инфраструктура на Министерството е дозволен само преку одобрени безбедносни механизми од Директоратот за комуникации и во согласност со утврдените безбедносни побарувања.

При користење на службената електронска пошта од надворешни и приватни уреди, корисниците се должни:

- да пристапуваат до службената електронска пошта само од службени уреди или од приватни уреди регистрирани и управувани преку систем за управување со мобилни уреди (Mobile Device Management – MDM);
- да користат повеќефакторска автентикација (MFA), кога таа е пропишана;
- да пристапуваат исклучиво преку одобрен VPN или друг безбеден механизам за далечински пристап;
- да не зачувуваат лозинки или други податоци за автентикација на уредот или во интернет-прелистувачот;
- да не пристапуваат до службената електронска пошта од јавни или споделени компјутери;
- да не преземаат, зачувуваат или обработуваат службени податоци на јавни компјутери;
- да не пристапуваат до класифицирани информации од приватни или јавни уреди, освен ако тоа не е изрично дозволено согласно важечките прописи и воспоставените безбедносни мерки и
- без одлагање да пријават секое сомневање за компромитирање на корисничката сметка, пристапните податоци или уредот.

5.4.Лозинки и автентикација

Член 10

Корисниците се должни да ги користат средствата за автентикација на начин што обезбедува соодветна заштита на корисничките сметки и информатичките системи.

Корисниците се должни:

- да користат лозинки што ги исполнуваат безбедносните барања утврдени со интерните политики;
- да не ги откриваат, споделуваат или отстапуваат лозинките и другите средства за автентикација на други лица;
- да ги менуваат лозинките во роковите утврдени со организациската политика или веднаш при сомневање дека се компромитирани;
- да користат повеќефакторска автентикација кога таа е овозможена или задолжителна и
- да не ги запишуваат лозинките на видливи места или на начин што овозможува нивно неовластено откривање.

Секој корисник е лично одговорен за сите активности извршени со користење на неговите средства за автентикација.

5.5.Користење на мобилни уреди

Член 11

Мобилните уреди доделени на користење се во сопственост на Министерство. Сите податоци зачувани во доделените службени мобилни уреди претставуваат сопственост на Министерството. Секој корисник пред добивање на мобилен уред на користење, потребно е да се запознае, разбере и прифати овие услови за користење на доделеното средство.

Службените мобилни уреди што се доделуваат на користење мора да бидат заштитени со соодветни механизми за автентикација, како што се PIN-код, лозинка, биометриска заштита или други одобрени безбедносни мерки.

Мобилните уреди мора да бидат конфигурирани на начин што обезбедува заштита на податоците, вклучително и примена на енкрипција на податоците складирани на уредот, како и овозможување на функции за далечинско заклучување и бришење при губење или кражба.

Корисниците се должни да ги заклучуваат мобилните уреди кога не се во употреба и да преземаат мерки за нивна заштита од неовластен пристап, губење или оштетување.

Секое губење, кражба или сомневање за компромитирање на службен мобилен уред мора без одлагање да се пријави до надлежната служба за информатичка безбедност или Service Desk, согласно интерните процедури.

5.6.Користење на надворешни медиуми за складирање и пренос на податоци

Член 12

Користењето на надворешни медиуми за складирање и пренос на податоци (USB уреди, надворешни хард дискови и други преносни медиуми) е дозволено исклучиво со претходно одобрение од надлежната организациска единица.

Сите надворешни медиуми мора да бидат проверени со одобрени безбедносни и антивирусни алатки, пред нивна употреба во информатичките системи на Министерството.

Се забранува користење на неовластени или непроверени надворешни медиуми во информатичките системи на Министерството.

5.7. Користење на услуги во облак

Член 13

Користењето на услуги во облак (cloud услуги) е дозволено исклучиво за услуги што се претходно одобрени од Министерството и кои ги исполнуваат безбедносните, техничките и правните барања утврдени со интерните акти.

Забрането е складирање, обработка или пренос на службени податоци на приватни или неовластени cloud-сметки и cloud сервиси.

При користење на одобрени cloud услуги, корисниците се должни да ги почитуваат мерките за заштита на податоците, контрола на пристап, автентикација и евиденција на активности, согласно безбедносните политики на Министерството.

5.8. Користење на генеративна вештачка интелигенција (AI)

Член 14

Користењето на алатки за генеративна вештачка интелигенција е дозволено исклучиво во согласност со интерните политики и безбедносни правила на Министерството.

Забрането е внесување, обработка или пренос на класифицирани, доверливи или чувствителни информации во јавни или неовластени ВИ системи.

Забрането е внесување лични податоци без соодветна правна основа и безбедносно одобрение.

Корисниците се должни да ги проверуваат резултатите добиени од AI алатки пред нивна службена употреба, при што целосната одговорност за точноста, законитоста и соодветноста на содржината останува на корисникот.

Користењето на AI алатки не смее да доведе до компромитирање на безбедноста, доверливоста или интегритетот на информатичките системи на Министерството.

5.9.Користење на социјални мрежи

Член 15

Корисниците се должни да ги користат социјалните мрежи согласно Етичкиот кодекс на вработените во Министерството за одбрана, Законот за класифицирани информации, Законот за служба во Армијата на Република Северна Македонија, Законот за вработените во Министерството за одбрана и во согласност со обврските за заштита на службените информации и угледот на Министерството.

Корисниците не смеат да објавуваат, споделуваат или пренесуваат службени, доверливи или класифицирани информации без претходно овластување.

Забрането е објавување фотографии, видео материјали или информации од заштитени службени простории, информациски системи или техничка опрема на Министерството.

Корисниците се должни да се воздржат од активности кои можат да го нарушат угледот, безбедноста или доверливоста на Министерството, или да доведат до откривање на службени информации.

Забрането е споделување содржини со класифицирани информации, воена опрема или детали што можат да ја загрозат безбедноста, а фотографии и видеа од активности на Министерството (вежби, конференции, состаноци и сл.) смеат да се објавуваат само со претходно одобрение од надлежна служба.

Службените профили на Министерството се единствени овластени канали за јавно споделување информации.

Корисниците се одговорни за содржината што ја објавуваат и мора да постапуваат во согласност со правилата за информатичка безбедност.

VI.МОНИТОРИНГ НА ИНФОРМАТИЧКИТЕ СИСТЕМИ И СРЕДСТВА

Член 16

Министерството го задржува правото да врши мониторинг, евиденција и анализа на користењето на информатичките системи, електронската пошта, интернет пристапот и другите информатички ресурси.

Мониторингот се спроведува во согласност со важечките законски и подзаконски прописи, како и интерните акти, а со цел заштита на информатичките системи, обезбедување на доверливоста, интегритетот и расположливоста на информациите, откривање и спречување на безбедносни инциденти, како и утврдување и истражување на злоупотреби.

VII.ПРИЈАВУВАЊЕ БЕЗБЕДНОСНИ ИНЦИДЕНТИ

Член 17

Корисниците се должни без одлагање да пријават секој безбедносен инцидент или сомневање за безбедносен инцидент, вклучително, но не ограничено на:

- сомнителни електронски пораки и обиди за фишинг;
- компромитирани или откриени лозинки;
- губење или кражба на информатичко средство;
- сомневање за присуство на малициозен софтвер;
- неовластен пристап до информациски системи;
- истекување или неовластено откривање на информации и
- секој друг настан што може да влијае врз безбедноста на информатичките системи.

Пријавувањето се врши до одговорните за информатичка безбедност Министерството преку е-пошта на cyber.k4@mod.gov.mk или преку Системот за ИТ Поддршка на Министерството за одбрана http://hd.mod.gov.mk/, е-пошта helpdesk@mod.gov.mk согласно воспоставените процедури на Министерството.

VIII.НЕПОЧИТУВАЊЕ НА ПРАВИЛНИКОТ

Член 18

Непочитувањето на одредбите на овој Правилник претставува повреда на интерните правила на Министерството за одбрана.

Во зависност од тежината на повредата, може да се применат следниве мерки:

- ограничување или укинување на пристапот до информатичките системи;
- поведување дисциплинска постапка;
- утврдување материјална одговорност и
- поведување прекршочна или кривична постапка, согласно важечките закони на Република Северна Македонија.

IX.ЗАВРШНИ ОДРЕДБИ

Член 19

Овој Правилник влегува во сила со денот на донесувањето.

Овој Правилник може да се ревидира по потреба, а особено во случај на значајни организациски, технички или законски измени кои влијаат врз информацисказа безбедност на Министерството.

Директоратот за комуникации/Секторот К4 – ИКТ, како организациска единица одговорна за планирањето, организирањето и спроведувањето на Правилникот за прифатливо користење, е должен да изработи детални процедури и инструкции за негова примена на информатичките системи и средствата на Министерството.

Напредните мерки и безбедносни механизми за модернизација на ИКТ на Министерството кои произлегуваат од овој Правилник, Директоратот за комуникации ќе ги имплементира преку реализација на навремени побарувања преку системот за Јавни набавки.

МИНИСТЕР ЗА ОДБРАНА
Владо Мисајловски