Врз основа на член 32 ставови (6) и (8), а во врска со член 11 став (1) точка 2), член 16 став (1) точки 2), 8), 20), 21) и 22), член 31, член 32 ставови (1), (2), (3) и (4), член 33, член 36 и член 41 став (2) од Законот за безбедност на мрежни и информациски системи („Службен весник на Република Северна Македонија" бр. 135/2025), директорот на Агенцијата за електронски комуникации донесе

ПРЕДЛОГ - ПРАВИЛНИК

ЗА ТЕХНИЧКИ И МЕТОДОЛОШКИ БАРАЊА ЗА МЕРКИТЕ ЗА УПРАВУВАЊЕ СО САЈБЕР БЕЗБЕДНОСНИ РИЗИЦИ ЗА СУШТИНСКИТЕ И ВАЖНИТЕ СУБЈЕКТИ ОД НАДЛЕЖНОСТ НА АГЕНЦИЈАТА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ ПРЕКУ MKD-CIRT

I. ОПШТИ ОДРЕДБИ

Член 1
(Предмет)

(1) Со овој правилник се утврдуваат техничките и методолошките барања за мерките за управување со сајбер безбедносни ризици кои претставуваат закана за мрежните и информациските системи на суштинските и важните субјекти од надлежност на Агенцијата за електронски комуникации преку Националниот центар за одговор на компјутерски инциденти — MKD-CIRT.

(2) Барањата од ставот (1) на овој член се однесуваат на субјектите од член 4 став (1) точки 1), 2) и 8), член 4 став (2) и член 4 став (3) од Законот, во делот во кој Агенцијата за електронски комуникации преку MKD-CIRT е надлежен орган согласно член 11 став (1) точка 2) од Законот.

(3) Овој правилник ги конкретизира минималните категории на мерки од член 32 став (3) од Законот, со различно ниво на интензитет и зрелост за суштинските и важните субјекти, согласно принципот на пропорционалност, нивото на ризик, големината, опфатот, изложеноста, веројатноста и сериозноста на можните инциденти.

Член 2
(Цел)

Целта на овој правилник е да обезбеди јасна, споредлива и надзорно применлива рамка за тоа кои технички и методолошки барања се задолжителни за суштинските субјекти, кои се задолжителни и кои се препорачани за важните субјекти, и кои барања претставуваат препорачани добри практики, со цел:

– одржување на соодветно ниво на безбедност на мрежните и информациските системи;

– намалување на веројатноста и влијанието на сајбер безбедносни инциденти;

– обезбедување континуитет на услугите што ги обезбедуваат суштинските и важните субјекти;

– создавање основа за стручен надзор од страна на надлежниот орган;

– усогласување со европските и меѓународните норми и релевантните технички спецификации.

Член 3
(Принцип на диференцирани барања)

(1) Сите суштински и важни субјекти се должни да преземат технички, оперативни и организациски мерки пропорционални на ризикот и усогласени со современите достигнувања.

(2) Суштинските субјекти применуваат задолжителни барања со повисоко ниво на зрелост, докази, тестирање и контрола, затоа што нивното нарушување може да предизвика сериозни последици по континуитетот на критични, јавни, економски, дигитални или инфраструктурни услуги.

(3) Важните субјекти применуваат задолжителни барања и препорачани барања. Препорачаните барања се применуваат кога тоа е соодветно според ризикот, изложеноста, видот на услугата, обработката на податоци, бројот на корисници, меѓузависностите или поединечна мерка на надлежниот орган.

(4) Барање означено како препорачано за важен субјект може да стане задолжително со поединечна мерка на надлежниот орган ако стручен надзор, значаен инцидент, повторлива неусогласеност или анализа на ризик покажат дека истото е неопходно за постигнување соодветно ниво на безбедност.

Член 4

(Ознаки за ниво на применливост)

Во овој правилник и во Прилогот 1 се користат следните ознаки:

Ознака	Значење	Примена
З	Задолжително барање	Се применува како задолжително барање за субјектот за кој е означено, со обем и докази сразмерни на неговиот статус, ризик и критичност.
П	Препорачано барање	Добра практика која се применува кога е соодветно и пропорционално, а може да стане задолжителна со поединечна мерка на надлежниот орган согласно Законот.

Член 5

(Однос со член 23 став (5) од Законот)

(1) Барањата од овој правилник кои се однесуваат на справување со инциденти, управување со кризи и координирано откривање на ранливости се применуваат во согласност со заедничките или стандардизирани практики, шемите за класификација и класификациите што ги утврдува MKD-CIRT согласно член 23 став (5) од Законот.

(2) Субјектите се должни, при воспоставување на своите политики, процедури, планови и технички контроли за инциденти, кризи и ранливости, да ги користат националните шеми и упатства утврдени од MKD-CIRT, особено во делот на:

– категоризација и сериозност на инциденти;

– ескалација и известување;

– TLP/режим на доверливост и размена на информации;

– процедури за справување со инциденти;

– координирано откривање на ранливости;

– комуникација со надлежниот орган и надлежниот тим за одговор на компјутерски инциденти.

Член 6

(Документирање и докази за усогласеност)

(1) Субјектите се должни да обезбедат докази за усогласеност со барањата од овој правилник, вклучувајќи политики, процедури, записи, извештаи, регистри, логови, планови, резултати од тестирања, ревизии, обуки и други релевантни документи.

(2) На барање на надлежниот орган, субјектот доставува докази за усогласеност во рок и формат определен со барањето, водејќи сметка за заштита на личните податоци, деловната тајна, класифицираните информации и безбедносно чувствителните информации.

II. ТЕХНИЧКИ И МЕТОДОЛОШКИ БАРАЊА ПО КАТЕГОРИИ

Член 7

(Анализа на ризикот и безбедноста на информациските системи)

Субјектите воспоставуваат формален процес за анализа на ризик, кој најмалку опфаќа дефинирање на опфат, идентификација на средства, услуги, закани, ранливости и зависности, процена на веројатност и влијание, третман на ризик и редовно преиспитување. Суштинските субјекти применуваат проширена, континуирана и раководно одобрена анализа, додека важните субјекти применуваат основна и пропорционална анализа со задолжително годишно ажурирање и ажурирање при значајни промени.

Деталните барања, нивото на применливост за суштинските и важните субјекти и индикативните докази за усогласеност се дадени во Прилог 1, кој е составен дел на овој правилник.

Член 8

(Справување со инциденти)

Субјектите воспоставуваат план и процедури за откривање, пријавување, анализа, ограничување, отстранување, обновување и пост-инцидентно учење. Барањата се применуваат во согласност со член 33 од Законот и со стандардизираните практики и класификациски шеми утврдени од MKD-CIRT согласно член 23 став (5) од Законот.

Деталните барања, нивото на применливост за суштинските и важните субјекти и индикативните докази за усогласеност се дадени во Прилог 1, кој е составен дел на овој правилник.

Член 9

(Континуитет на работењето, обновување по катастрофален испад и управување со кризи)

Субјектите воспоставуваат процеси за континуитет на работењето, резервни копии, обновување по катастрофален испад и кризна комуникација. Суштинските субјекти применуваат проширено тестирање, формално управување со кризи и понапредни цели RTO/RPO, додека важните субјекти применуваат основни документирани планови и тестирање сразмерно на ризикот.

Деталните барања, нивото на применливост за суштинските и важните субјекти и индикативните докази за усогласеност се дадени во Прилог 1, кој е составен дел на овој правилник.

Член 10

(Безбедност на ланецот на снабдување)

Субјектите управуваат со ризиците од добавувачи, изведувачи, даватели на ИКТ услуги и други трети страни. Суштинските субјекти задолжително класифицираат критични добавувачи, спроведуваат длабинска проверка и договорни безбедносни клаузули; важните субјекти задолжително ги применуваат основните договорни и мониторинг барања, а проширените барања кога добавувачот е високоризичен.

Деталните барања, нивото на применливост за суштинските и важните субјекти и индикативните докази за усогласеност се дадени во Прилог 1, кој е составен дел на овој правилник.

Член 11

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

Субјектите вградуваат безбедносни барања во набавката, развојот, конфигурацијата, одржувањето и управувањето со ранливости. Суштинските субјекти применуваат построги рокови за санирање

ранливости, безбедносно тестирање и управување со промени, додека важните субјекти применуваат основни барања и проширени контроли за јавнодостапни или критични системи.

Деталните барања, нивото на применливост за суштинските и важните субјекти и индикативните докази за усогласеност се дадени во Прилог 1, кој е составен дел на овој правилник.

Член 12

(Политики и постапки за процена на ефикасноста на мерките)

Субјектите воспоставуваат политики, процедури, метрики, записи и механизми за проверка дали мерките за управување со сајбер безбедносни ризици функционираат. Суштинските субјекти применуваат редовни независни или внатрешно независни проверки, додека важните субјекти применуваат периодични проверки и таргетирани проверки кога тоа го бара ризикот или надлежниот орган.

Деталните барања, нивото на применливост за суштинските и важните субјекти и индикативните докази за усогласеност се дадени во Прилог 1, кој е составен дел на овој правилник.

Член 13

(Основни практики на сајбер хигиена и обуки)

Субјектите обезбедуваат основни практики на сајбер хигиена, редовно ажурирање, безбедно користење на уреди, заштита од фишинг, обука на вработени и механизам за пријавување сомнителни активности. Обуката е задолжителна за двата типа субјекти, со повисок интензитет, вежби и симулации кај суштинските субјекти.

Деталните барања, нивото на применливост за суштинските и важните субјекти и индикативните докази за усогласеност се дадени во Прилог 1, кој е составен дел на овој правилник.

Член 14

(Криптографски техники и шифрирање)

Субјектите применуваат соодветни криптографски техники за заштита на податоците во мирување и при пренос, управување со клучеви и забрана на застарени алгоритми. Суштинските субјекти применуваат проширено управување со клучеви и понапредна заштита за критичните системи и чувствителните податоци.

Деталните барања, нивото на применливост за суштинските и важните субјекти и индикативните докази за усогласеност се дадени во Прилог 1, кој е составен дел на овој правилник.

Член 15

(Безбедност на човечки ресурси, контрола на пристап и управување со средства)

Субјектите воспоставуваат политики за животен циклус на пристап, контрола на привилегии, управување со кориснички сметки, безбедносни проверки за критични улоги и инвентар на средства. Суштинските субјекти применуваат почести ревизии и построги контроли за привилегиран пристап.

Деталните барања, нивото на применливост за суштинските и важните субјекти и индикативните докази за усогласеност се дадени во Прилог 1, кој е составен дел на овој правилник.

Член 16

(Повеќе-факторска автентикација и безбедни комуникации)

Субјектите применуваат повеќе-факторска автентикација за привилегиран, далечински и друг високоризичен пристап, како и безбедни говорни, видео и текстуални комуникации и алтернативни канали за итни случаи. Суштинските субјекти применуваат проширени барања за фишинг-отпорна автентикација и посебни канали за кризна комуникација.

Деталните барања, нивото на применливост за суштинските и важните субјекти и индикативните докази за усогласеност се дадени во Прилог 1, кој е составен дел на овој правилник.

III. НАДЗОР, ПРИМЕНА И АЖУРИРАЊЕ

Член 17

(План за усогласување)

(1) Субјектите кои не ги исполнуваат барањата од овој правилник се должни да изготват план за усогласување кој ги содржи утврдените недостатоци, корективните мерки, одговорните лица и роковите за реализација.

(2) При утврдување на роковите од ставот (1), субјектите го земаат предвид нивото на ризик, критичноста на услугата и потребата за итно намалување на сајбер безбедносниот ризик.

Член 18

(Надзор и корективни мерки)

Надлежниот орган, при вршење стручен надзор, ја оценува усогласеноста на субјектот со барањата од овој правилник, при што може да побара докази, да наложи корективни мерки, да утврди рокови за усогласување и да преземе други мерки согласн

о Законот.

Член 19

(Ажурирање на барањата)

(1) Барањата од овој правилник се преиспитуваат најмалку еднаш годишно или при значајни промени во заканите, технологиите, европските и меѓународните норми, националните стандарди, шемите за класификација или искуствата од значајни сајбер безбедносни инциденти.

(2) MKD-CIRT може да издава упатства, образци, контролни листи и технички насоки за практична примена на овој правилник, кои не смеат да бидат во спротивност со овој правилник и Законот.

IV. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 20

(Преодна примена)

(1) Субјектите кои на денот на влегувањето во сила на овој правилник веќе имаат воспоставени политики, процедури и технички контроли, ги усогласуваат истите со овој правилник при првото редовно ажурирање, а најдоцна во рок од шест месеци од денот на влегувањето во сила.

(2) Кога субјектот е дополнително утврден како суштински или важен субјект, рокот од ставот (1) започнува да тече од денот на известувањето за неговиот статус, освен ако со поединечен акт или мерка на надлежниот орган не е утврден пократок рок поради висок ризик.

Член 21

(Влегување во сила)

(1)Правилникот за технички и методолошки барања за мерките за управување со сајбер безбедносни ризици за суштинските и важните субјекти од надлежност на Агенцијата за електронски комуникации преку MKD-CIRT започува да се применува со денот на објавувањето во „Службен весник на Република Северна Македонија".

По влегувањето во сила, овој Правилник ќе биде објавена и на веб страната на Агенцијата за електронски комуникации.

Бр. 01 01 - 1513 /14

14.07. 2026 година

Скопје

Директор

на Агенцијата за електронски комуникации

Nusret Haliti

Изготвил:

Раководител на MKD-CIRT
Sevdali Selmani

ПРИЛОГ 1

МАТРИЦА НА ТЕХНИЧКИ И МЕТОДОЛОШКИ БАРАЊА ЗА СУШТИНСКИ И ВАЖНИ СУБЈЕКТИ

Овој прилог ја определува применливоста на барањата. Ознаките З и П се толкуваат согласно член 4 од овој правилник.

Категорија	Барање	Методолошко барање	Технички доказ/контрола	Суштински	Важни	Напомена
1. Анализа на ризик	1.1 Опфат и контекст на проценката	Да се дефинираат услуги, системи, процеси, податоци, локации и трети страни што се предмет на проценката.	Документиран опфат, методологија, мапа на услуги и системи.	З	З	За суштински субјект опфатот мора да ги вклучи сите критични услуги и меѓузависности.
1. Анализа на ризик	1.2 Инвентар и класификација на средства	Да се води ажуриран инвентар на хардвер, софтвер, податоци, услуги, сметки, облак ресурси и мрежни сегменти.	CMDB/инвентар, сопственик на средство, критичност, локација, статус.	З	З	За суштински субјекти ажурирањето е континуирано или најмалку квартално; за важни најмалку годишно и при промена.
1. Анализа на ризик	1.3 Идентификација на закани и ранливости	Да се идентификуваат релевантни закани, ранливости и вектори на напад.	Скенирања, извештаи, threat intelligence, CVE/CVSS, MITRE ATT&CK мапирање кога е применливо.	З	З	За важни субјекти MITRE мапирањето е задолжително кога се работи за значајни или повторливи инциденти.
1. Анализа на ризик	1.4 Оценка на ризик	Да се оценат веројатност, влијание, постојни контроли и преостанат ризик.	Матрица на ризик, ризик-регистар, оценка CIA, критериуми за прифаќање.	З	З	Субјектот мора да има јасна скала и критериуми.
1. Анализа на ризик	1.5 План за третман на ризици	Да се утврдат мерки за ублажување, избегнување, трансфер или прифаќање на ризик.	План со сопственик, рок, приоритет, статус и доказ за реализација.	З	З	Прифаќање висок ризик кај суштински субјект мора да биде одобрено од највисоко раководство.
1. Анализа на ризик	1.6 Редовен преглед	Проценката на ризик да се ажурира најмалку еднаш годишно и по значајна промена.	Записник/одлука на орган на управување, ажуриран регистар на ризици.	З	З	Усогласено со член 31 од Законот.
1. Анализа на ризик	1.7 Континуирано следење на ризик	Да се воспостави механизам за следење на нови закани, ранливости, изложеност и промени.	Vulnerability management, ASM, SIEM извештаи, логови, известувања од MKD-CIRT.	З	З	Кај важни субјекти задолжително е за јавно достапни и критични системи; за останати системи се применува пропорционално.
2. Справување со инциденти	2.1 План за одговор на инциденти	Да се воспостави писмен план со улоги, есхалација, комуникација, критериуми за сериозност и затворање.	IRP, матрица на улоги, контакти, процедури, одобрение од раководство.	З	З	Мора да биде усогласен со националните шеми на MKD-CIRT по член 23(5).
2. Справување со инциденти	2.2 Детекција и иницијална анализа	Да се обезбедат процеси за откривање, валидација и иницијална процена на инциденти.	Логирање, мониторинг, IDS/EDR/SIEM или еквивалент, процедури за тријажа.	З	З	За важни субјекти алатките се пропорционални на ризикот и големината.
2. Справување со инциденти	2.3 Законско известување	Да се обезбеди способност за пријавување согласно роковите од член 33 од Законот.	Процедура за 3 часа, 24 часа, 72 часа, привремено и завршно известување.	З	З	Ова е задолжително за двата типа субјекти.
2. Справување со инциденти	2.4 Ограничување, отстранување и обновување	Да се дефинираат технички дејства за containment, eradication и recovery.	Playbooks, мрежна изолација, rollback, backup restore, промена на кредeнцијали.	З	З	За суштински субјекти се бараат сценарија за повеќе типови инциденти.
2. Справување со инциденти	2.5 Форензичко зачувување	Да се зачуваат релевантни докази кога е применливо.	Логови, хеш-вредности, chain of custody, временски печати.	З	З	Кај важни субјекти задолжително е за значајни инциденти, сомневање за кривично дело или барање на надлежниот орган.

2. Справување со инциденти	2.6 Вежби и тестирања	Да се тестира планот за одговор на инциденти.	Table-top/технички вежби, извештаи, научени поуки.	З	П	Кај важни субјекти станува З ако обезбедуваат јавнодостапна или високо зависна услуга.
3. Континуитет и кризи	3.1 Анализа на влијание врз работењето	Да се идентификуваат критични функции, услуги, системи, зависности и приоритети за обновување.	BIA, листа на критични услуги, сопственици, зависности.	З	З	За суштински субјекти BIA мора да биде сеопфатна и одобрена од раководството.
3. Континуитет и кризи	3.2 RTO/RPO цели	Да се утврдат цели за време на обновување и точка на обновување.	RTO/RPO по услуга, одлука за прифатлив прекин, SLA/OLA.	З	З	За важни субјекти може да биде поедноставено но мора да биде документирано.
3. Континуитет и кризи	3.3 Резервни копии	Да се обезбеди редовна, тестирана и заштитена резервна копија.	Backup политика, immutable/offline копии, тестови за restore.	З	З	Суштинските субјекти применуваат најмалку една изолирана или непроменлива копија за критични системи.
3. Континуитет и кризи	3.4 DR/BCP планови	Да се воспостават планови за обновување по катастрофален испад и континуитет на работењето.	DRP/BCP, процедури, контакти, алтернативни локации/ресурси.	З	З	За важни субјекти опфатот е пропорционален на критичните услуги.
3. Континуитет и кризи	3.5 Управување со кризи	Да се воспостави кризна структура и комуникациски план за големи инциденти.	Кризен тим, матрица за ескалација, комуникациски сценарија.	З	П	За важни субјекти задолжително ако прекинот може да влијае врз повеќе субјекти или корисници. За важни субјекти ова барање е препорачано, а може да биде задолжително со поединечна мерка на надлежниот орган или кога тоа произлегува од проценка на ризик.
3. Континуитет и кризи	3.6 Тестирање на планови	Да се тестираат BCP/DR плановите.	Годишни тестови за суштински; најмалку периодични или по промена за важни.	З	П	Надлежниот орган може да наложи тест по значаен инцидент. За важни субјекти ова барање е препорачано, а може да биде задолжително со поединечна мерка на надлежниот орган или кога тоа произлегува од проценка на ризик.
4. Ланец на снабдување	4.1 Регистар на добавувачи	Да се води регистар на добавувачи, даватели на услуги, облак, дата центар и управувани услуги.	Регистар со критичност, услуга, договор, контакт, зависност.	З	З	Клучно за B2B ИКТ и дигитална инфраструктура.
4. Ланец на снабдување	4.2 Класификација на добавувачи по ризик	Да се класифицираат добавувачите според пристап, критичност, податоци и зависност.	Risk tiering, процена пред договор, годишен преглед.	З	З	Кај важни субјекти може да се применува само за критични добавувачи.
4. Ланец на снабдување	4.3 Договорни безбедносни клаузули	Договорите да содржат барања за безбедност, инциденти, пристап, податоци и раскинување.	Клаузули за известување, audit right, минимални контроли, подизведувачи.	З	З	Задолжително за нови договори и при обновување на постојни.
4. Ланец на снабдување	4.4 Длабинска проверка	Да се спроведе безбедносна проверка пред избор на критичен добавувач.	Прашалник, сертификати, извештаи, резултати од ревизија.	З	З	За важни субјекти задолжително за високоризични добавувачи.
4. Ланец на снабдување	4.5 Известување од добавувач	Добавувачот да известува за инциденти кои можат да влијаат врз субјектот.	Договорна SLA клаузула, контакт точка, процедура за ескалација.	З	З	Мора да овозможи навремено исполнување на член 33.
4. Ланец на снабдување	4.6 Престанок на договор и одземање пристап	Да се уредат процедури за враќање на средства, податоци и одземање пристап.	Termination checklist, revocation logs, data deletion certificate.	З	З	Се применува за сите даватели со пристап до системи или податоци.
5. Набавка/развој/одржување	5.1 Безбедносни барања во набавка	Да се вградат безбедносни барања во технички спецификации и договори.	Security-by-design барања, минимални стандарди, проверка пред прием.	З	З	Се применува за ИКТ услуги, системи и производи.

5. Набавка/развој/одржување	5.2 Безбедна конфигурација	Да се користат безбедносни baseline конфигурации и hardening.	CIS/еквивалентни baseline, configuration management, evidence of hardening.	З	З	За важни субјекти најмалку за критични и интернет-достапни системи.
5. Набавка/развој/одржување	5.3 Управување со ранливости	Да се идентификуваат, оценуваат, приоритизираат и санираат ранливости.	Скенирања, CVSS/контекст, ticketing, SLA за санација.	З	З	Индикативно: суштински — критични 72 ч./високи 14 дена; важни — критични 7 дена/високи 30 дена, освен ако ризикот бара побрзо.
5. Набавка/развој/одржување	5.4 Управување со закрпи	Да се воспостави процес за безбедносни ажурирања и итни закрпи.	Patch policy, тестирање, rollback, извештаи за применети закрпи.	З	З	За критични ранливости се применува итна постапка.
5. Набавка/развој/одржување	5.5 Безбеден развој	Кога субјектот развива софтвер, да применува secure SDLC.	Threat modeling, code review, SAST/DAST, dependency scanning.	З	З	Задолжително е за субјекти кои развиваат или значително модифицираат софтвер; за субјекти без развојна функција се применува преку барања кон добавувачите.
5. Набавка/развој/одржување	5.6 Пенетрациско тестирање	Да се врши тестирање на изложени и критични системи.	Извештаи од тестирање, remediation plan, retest.	З	З	За важни субјекти задолжително е за критични јавнодостапни системи и по значајна промена; за останатите системи е препорачано.
5. Набавка/развој/одржување	5.7 Управување со промени	Да се контролираат промени на продукциски системи.	Change records, approvals, rollback, emergency change procedure.	З	З	Се применува за сите продукциски системи.
6. Процена на ефикасност	6.1 Политики и процедури	Да се усвојат политики и процедури за сајбер безбедност, одобрени од раководство.	Политики, верзии, одобренија, ревизии.	З	З	Суштинските субјекти применуваат целосен систем на политики.
6. Процена на ефикасност	6.2 Рамка или стандард	Да се усогласи управувањето со призната рамка/стандард.	ISO/IEC 27001, NIST CSF, CIS Controls или еквивалентна мапа.	З	П	За важни субјекти е препорачано, а може да биде задолжително со поединечна мерка на надлежниот орган при висок ризик.
6. Процена на ефикасност	6.3 Внатрешна проверка	Да се врши периодична проверка на примената на мерките.	Checklists, internal audit reports, evidence review.	З	З	Најмалку годишно за двата типа; кај суштински може и почесто.
6. Процена на ефикасност	6.4 Независна проверка/ревизија	Да се обезбеди независна процена кога ризикот или надлежниот орган го бара тоа.	Извештај од независен ревизор, remedial plan.	З	П	Кај важни субјекти задолжително по барање на надлежниот орган или по значаен инцидент. За важни субјекти ова барање е препорачано, а може да биде задолжително со поединечна мерка на надлежниот орган или кога тоа произлегува од проценка на ризик.
6. Процена на ефикасност	6.5 Логирање и мониторинг	Да се евидентираат безбедносни настани и да се следат аномалии.	Лог политика, retention, SIEM/централизирани логови, alerting.	З	З	За важни субјекти централизацијата е пропорционална на системите и ризикот.
6. Процена на ефикасност	6.6 Следење на корективни мерки	Да се следи реализацијата на мерките од ревизии, тестови и инциденти.	Action tracker, owners, deadlines, status reports.	З	З	Неисполнети мерки со висок ризик се ескалираат до раководството.
7. Сајбер хигиена и обуки	7.1 Годишна обука	Да се обезбеди редовна обука за сите вработени и релевантни ангажирани лица.	Програма, присуство, тестови, материјали.	З	З	Минимум еднаш годишно и при вработување.
7. Сајбер хигиена и обуки	7.2 Специјализирана обука	Да се обучат лица со улоги во ИКТ, безбедност, инциденти и управување.	Сертификати, план за обука, евиденција.	З	П	За важни субјекти задолжително кога има назначени технички/безбедносни улоги. За важни субјекти ова барање е препорачано, а може да биде задолжително со поединечна мерка на надлежниот орган или кога тоа произлегува од проценка на ризик.

7. Сајбер хигиена и обуки	7.3 Фишинг и социјално инженерство	Да се спроведуваат мерки за препознавање и пријавување фишинг.	Обучувања, симулации, известувања, mail security controls.	З	З	Симулации се задолжителни за суштински, препорачани за важни.
7. Сајбер хигиена и обуки	7.4 Политики за лозинки и уреди	Да се уредат лозинки, користење уреди, removable media, BYOD и ажурирања.	Policies, MDM/endpoint controls, patch reports.	З	З	Се применува за сите корисници.
7. Сајбер хигиена и обуки	7.5 Пријавување сомнителни активности	Да постои лесен механизам за внатрешно пријавување.	Контакт точка, mailbox/ticket, инструкции за корисници.	З	З	Механизмот мора да води до одговорното лице/тим.
8. Криптографија	8.1 Класификација на податоци	Да се класифицираат податоците и да се утврди ниво на заштита.	Data classification policy, labels, mapping to controls.	З	З	Претходен услов за правилна енкрипција.
8. Криптографија	8.2 Енкрипција при пренос	Да се користат безбедни протоколи за пренос на податоци.	TLS 1.2+/1.3, VPN/IPsec, S/MIME или еквивалент, сертификати.	З	З	Застарени протоколи се исклучуваат или документирано се ограничуваат.
8. Криптографија	8.3 Енкрипција во мирување	Да се шифрираат чувствителни, доверливи и критични податоци.	Full disk/database encryption, encrypted backups.	З	З	Кај важни субјекти најмалку за чувствителни и критични податоци.
8. Криптографија	8.4 Управување со клучеви	Да се уреди генерирање, чување, ротација, пристап и уништување на клучеви.	Key management policy, access logs, KMS/HSM when applicable.	З	П	HSM/KMS е задолжително за критични клучеви кај суштински субјекти, а препорачано за важни субјекти освен кога ризикот бара поинаку. За важни субјекти ова барање е препорачано, а може да биде задолжително со поединечна мерка на надлежниот орган или кога тоа произлегува од проценка на ризик.
8. Криптографија	8.5 Забрана на слаби алгоритми	Да се исклучат застарени и небезбедни алгоритми.	Crypto policy, scanning reports, configuration evidence.	З	З	DES, RC4, SSL и други небезбедни механизми не се користат.
9. HR, пристап и средства	9.1 HR безбедносни процедури	Да се уредат безбедносни обврски пред, за време и по престанок на ангажман.	Onboarding/offboarding checklist, NDA, role obligations.	З	З	Се применува и за надворешни лица со пристап.
9. HR, пристап и средства	9.2 Безбедносна проверка за привилегирани улоги	Да се врши проверка сразмерна на ризикот за лица со привилегиран пристап.	Проверка, изјава, одобрение, ревизиска трага.	З	П	Кај важни субјекти задолжително за критични системи и чувствителни податоци. За важни субјекти ова барање е препорачано, а може да биде задолжително со поединечна мерка на надлежниот орган или кога тоа произлегува од проценка на ризик.
9. HR, пристап и средства	9.3 Управување со идентитети и пристап	Да се применуваат least privilege, segregation of duties и одобрување на пристап.	IAM records, approvals, access matrix, privileged access management.	З	З	За суштински субјекти PAM е препорачана напредна контрола, а за администраторски сметки се применува задолжително управување со привилегиран пристап.
9. HR, пристап и средства	9.4 Ревизија на пристапи	Да се ревидираат сметки и права на пристап.	Quarterly/annual reviews, revocation evidence.	З	З	Суштински најмалку квартално за привилегирани сметки; важни најмалку годишно.
9. HR, пристап и средства	9.5 Инвентар и животен циклус на средства	Да се следат средствата од набавка до отстранување.	Asset lifecycle records, ownership, disposal certificates.	З	З	Поврзано со член 7.1 од матрицата.
9. HR, пристап и средства	9.6 Безбедно отстранување	Да се обезбеди безбедно бришење/уништување на податоци и средства.	Wiping certificates, destruction records, reuse procedure.	З	З	Се применува при престанок, замена или реупотреба.
10. MFA и комуникации	10.1 MFA за привилегиран пристап	Да се користи MFA за администраторски и привилегирани сметки.	MFA policy, configuration evidence, exception records.	З	З	Без исклучок, освен документарно оправдан break-glass режим.

10. MFA и комуникации	10.2 MFA за далечински пристап	Да се користи MFA за VPN, remote desktop, cloud admin и други далечински пристапи.	VPN/IdP configuration, logs, access policy.	З	З	Се применува за сите корисници со далечински пристап.
10. MFA и комуникации	10.3 MFA за е-пошта и облачни услуги	Да се применува MFA за корпоративна е-пошта и облачни услуги.	IdP policy, conditional access, MFA reports.	З	П	За важни субјекти задолжително ако користат cloud/email за деловни или чувствителни податоци. За важни субјекти ова барање е препорачано, а може да биде задолжително со поединечна мерка на надлежниот орган или кога тоа произлегува од проценка на ризик.
10. MFA и комуникации	10.4 Фишинг-отпорна автентикација	Да се користат FIDO2, smart card или еквивалент за најризични сметки.	Hardware keys/smart cards, policy, enrollment logs.	З	П	Задолжително за суштински субјекти за администраторски и критични улоги.
10. MFA и комуникации	10.5 Безбедни комуникации со надлежни органи и MKD-CIRT	Да се обезбедат доверливи канали за размена на информации за инциденти и закани.	PGP/S/MIME, secure portal, TLP procedure, contact list.	З	З	Мора да биде усогласено со шемите на MKD-CIRT по член 23(5).
10. MFA и комуникации	10.6 Итни комуникации	Да се обезбедат алтернативни комуникациски канали за кризни состојби.	Emergency contacts, out-of-band channel, crisis comms test.	З	П	Кај важни субјекти задолжително ако услугата има голема зависност од јавни мрежи. За важни субјекти ова барање е препорачано, а може да биде задолжително со поединечна мерка на надлежниот орган или кога тоа произлегува од проценка на ризик.
10. MFA и комуникации	10.7 Следење на автентикација и комуникации	Да се следат неуспешни најави, ризични најави, промени на MFA и сомнителна комуникација.	Logs, alerts, SIEM/use-case reports, incident tickets.	З	З	Кај важни субјекти може да биде централизирано или локално, сразмерно на ризикот.

ПРИЛОГ 2
КРАТКО РЕЗИМЕ НА РАЗЛИКИТЕ МЕЃУ СУШТИНСКИ И ВАЖНИ СУБЈЕКТИ

Област	Суштински субјекти	Важни субјекти
Општ стандард	Целосна и проширена примена на барањата; повисока зрелост, почесто тестирање и посилна документација.	Основна и пропорционална примена; дополнителни препорачани мерки кога ризикот, услугата или надлежниот орган го бараат тоа.
Надзорна логика	Поголема подготвеност за проактивен и ex post надзор, ревизии, барања за докази и корективни мерки.	Првенствено усогласеност со основни барања и ex post/ризик-базиран надзор.
Инциденти	Формален IRP, вежби, брза ескалација, форензичко зачувување и усогласеност со националните шеми на MKD-CIRT.	IRP и пријавување се задолжителни; вежби и форензичка зрелост се прошируваат според ризикот.
Континуитет	BIA, RTO/RPO, DR/BCP, кризна комуникација и редовно тестирање.	Документирани планови и тестирање сразмерно на критичноста и ризикот.
Технички контроли	Побрзи рокови за ранливости, посилно мониторирање, MFA за високоризични сметки, напредно управување со клучеви.	Минимални задолжителни контроли, со препорачано дополнително проширување за критични/јавнодостапни системи.