

Врз основа на член 191 став (5), а во врска со член 197 од Законот за електронските комуникации („Службен весник на Република Северна Македонија“ бр. 135/2025, 269/2025 и 132/2026), директорот на Агенцијата за електронски комуникации, и директорот на Агенцијата за заштита на личните податоци, на ден ____ / ____ / ____ година, донесоа

ПРЕДЛОГ - ПРАВИЛНИК ЗА ОБЕЗБЕДУВАЊЕ НА БЕЗБЕДНОСТ И ИНТЕГРИТЕТ НА ЈАВНИТЕ ЕЛЕКТРОНСКИ КОМУНИКАЦИСКИ МРЕЖИ И УСЛУГИ И АКТИВНОСТИТЕ ШТО ОПЕРАТОРИТЕ ТРЕБА ДА ГИ ПРЕЗЕМААТ ПРИ НАРУШУВАЊЕ НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ*

I. ОСНОВНИ ОДРЕДБИ

Член 1

(1) Со овој правилник се пропишуваат:

- 1) начинот на кој операторите се должни да обезбедат безбедност и интегритет на јавните електронски комуникациски мрежи и услуги и да ги спроведат одредбите од член 191 од Законот за електронските комуникации, преку задолжителни инструкции;
- 2) формата, содржината и начинот на доставување на известувањата утврдени со членовите 191 и 197 од Законот за електронските комуникации;
- 3) начинот на постапување на Агенцијата за електронски комуникации во врска со добиените известувања за нарушување на безбедноста или губење на интегритетот на мрежите или услугите;
- 4) активностите што операторите треба да ги преземат при нарушување на безбедноста на личните податоци;
- 5) начинот на доставување на политиката за безбедност, самопроцената и другата потребна документација по барање на Агенцијата за електронски комуникации и
- 6) формата и содржината на регистарот на нарушувањата на безбедноста на личните податоци и начинот на неговото водење.

Член 2

(1) Во овој правилник, покрај изразите утврдени во Законот за електронските комуникации, Законот за безбедност на мрежни и информациски системи и прописите за заштита на личните податоци, се употребуваат и следниве изрази:

- 1) **„информациски систем“** е комуникациски, компјутерски или друг електронски систем преку кој операторот ги обезбедува услугите од член 11 од овој правилник;
- 2) **„безбедносен инцидент“** е нарушување на безбедноста што има значително влијание врз работењето на електронската комуникациска мрежа или услуга;
- 3) **„интегритет на јавните електронски комуникациски мрежи“** е способност на системот да ги зачува специфичните карактеристики во однос на перформансите и функционалностите;
- 4) **„информациска безбедност“** е зачувување на доверливоста, интегритетот и достапноста на информациите, согласно ISO/IEC 27001 и

*Со овој правилник се врши усогласување со Директивата 2002/58/EЗ на Европскиот парламент и на Советот од 12 јули 2002 година за обработката на личните податоци и заштитата на приватноста во секторот на електронските комуникации и со Регулативата (ЕУ) бр. 611/2013 на Комисијата од 24 јуни 2013 година за мерките што се применуваат при известување за нарушување на безбедноста на личните податоци согласно со Директивата 2002/58/EЗ.

- 5) „безбедност на јавните електронски комуникациски мрежи“ е зачувување на доверливоста, интегритетот и достапноста на мрежите, како дел од информациската безбедност.

II. ТЕХНИЧКИ, ОПЕРАТИВНИ И ОРГАНИЗАЦИСКИ МЕРКИ ШТО ОПЕРАТОРИТЕ ТРЕБА ДА ГИ ПРЕЗЕМААТ ВО ОДНОС НА БЕЗБЕДНОСТА И ИНТЕГРИТЕТОТ НА ЈАВНИТЕ ЕЛЕКТРОНСКИ КОМУНИКАЦИСКИ МРЕЖИ И УСЛУГИ

Член 3

(1) Операторите се должни да извршат проценка на ризиците за информациската безбедност на мрежите и услугите, како и за обработката на личните податоци, и врз основа на процената да преземаат соодветни технички, оперативни и организациски мерки за управување со утврдените ризици.

(2) Мерките од ставот (1) на овој член треба да бидат пропорционални на утврдениот ризик, имајќи ги предвид: техничкиот напредок, големината, сложеноста и изложеноста на операторот и да обезбедат ниво на безбедност соодветно на ризикот.

(3) Мерките особено треба да го спречат и да го сведат на најмала можна мера влијанието на безбедносните инциденти врз корисниците и меѓусебно поврзаните мрежи.

(4) Процената на ризиците и мерките од овој член се спроведуваат согласно прописите со кои се уредува безбедноста на мрежни и информациски системи, со примена на релевантните стандарди, особено ISO/IEC 27001 и релевантните препораки на ENISA. Мерките што се однесуваат на безбедноста на обработката на личните податоци операторите се должни да ги усогласат и со прописите за заштита на личните податоци.

Член 4

(1) Операторите се должни да ги преземаат сите соодветни чекори за да го обезбедат интегритетот на своите мрежи и истовремено континуитетот на услугите што ги обезбедуваат со тие мрежи.

(2) Со преземените чекори од ставот (1) на овој член треба да се постигне степен на сигурност што одговара на постојните закани, да се спречат безбедносни инциденти и да се ублажи нивното влијание врз работењето на јавните електронски комуникациски мрежи и услуги.

Член 5

Заради спроведување на членовите 3 и 4 од овој правилник, операторите се должни да усвојат и да имплементираат политика за безбедност со која се утврдуваат ранливоста на системот, надзорот и спроведувањето на превентивни и корективни мерки, како и мерки за ублажување на инцидентите по безбедноста и интегритетот на мрежите, согласно прописите со кои се уредува безбедноста на мрежни и информациски системи.

Член 6

(1) Политиката за безбедност од членот 5 од овој правилник ги опфаќа најмалку:

- анализа и управување со ризиците;
- безбедност на човечките ресурси, контрола на пристап и управување со средствата;
- физичка безбедност на системите и објектите;
- безбедност на обработката на личните податоци;
- оперативна безбедност, безбедност на синцирот на снабдување и управување со ранливостите;
- управување со инциденти;
- деловен континуитет, резервни копии, обновување и кризен менаџмент;
- следење, тестирање и оценување на ефективност на мерките и
- сајбер-хигиена, обуки, криптографија и автентикација.

(2) Операторите ги применуваат минималните секторски безбедносни мерки од Прилогот 4, кој е составен дел на овој правилник, сразмерно со проценетиот ризик, големината и сложеноста на мрежите и услугите.

(3) Референтните стандарди се наведени во Прилог 5, кој е составен дел на овој правилник. Операторите можат да применуваат и други стандарди со кои се постигнува еднакво или повисоко ниво на безбедност.

(4) Политиката и документацијата за периодичната самооценка се чуваат кај операторот и се доставуваат до Агенцијата по образложено барање. Проверка спроведена согласно прописите за безбедност на мрежни и информациски системи се признава доколку ги опфаќа барањата од овој правилник.

III. ИЗВЕСТУВАЊА ЗА НАСТАНАТИ НАРУШУВАЊА НА БЕЗБЕДНОСТА ИЛИ ГУБЕЊЕ НА ИНТЕГРИТЕТОТ НА МРЕЖИТЕ И УСЛУГИТЕ

Член 7

(1) Во случај на нарушување на безбедноста или губење на интегритетот што има значително влијание врз функционирањето на мрежите или услугите, операторите постапуваат согласно член 191 став (4) од Законот за електронските комуникации и го доставуваат известувањето на начин и во роковите утврдени со прописите со кои се уредува безбедноста на мрежни и информациски системи.

(2) Известувањето од ставот (1) на овој член се доставува по електронски пат, преку безбедниот канал за пријавување објавен од Агенцијата за електронски комуникации.

(3) Доколку нарушувањето на безбедноста може негативно да влијае врз корисниците од други држави, Агенцијата за електронски комуникации може да ги извести националните регулаторни тела на засегнатите држави.

(4) Агенцијата за електронски комуникации може за нарушувањето да ја извести Агенцијата на Европската Унија за сајбер-безбедност (ENISA), согласно закон и применливите правила за размена на информации.

(5) Кога се исполнети условите утврдени со закон, Агенцијата за електронски комуникации може да ја извести јавноста или да побара од операторот да го стори тоа.

Член 8

Агенцијата за електронски комуникации може да подготви годишен збирен извештај за добиените известувања и за преземените активности од член 7 од овој правилник и да го достави до ENISA согласно закон и насоките за известување на ENISA.

Член 9

(1) Во случај на сериозна сајбер-закана што може да влијае врз корисниците, операторот, без проценка дали информирањето е од јавен интерес, ги информира корисниците веднаш, а најдоцна во рокот утврден со прописите со кои се уредува безбедноста на мрежни и информациски системи.

(2) Доколку заканата е надвор од опсегот на мерките што ги презема операторот, информирањето од ставот (1) на овој член ги содржи можните решенија за отстранување на ризикот и можните трошоци за тие решенија.

(3) Операторот ги информира корисниците на еден или повеќе од следниве начини:

- 1) преку својата веб-страница;
- 2) преку сопствен телевизиски канал;
- 3) со електронска порака;
- 4) со СМС-порака или
- 5) преку други медиуми за јавно информирање.

Член 10

(1) За проценка на оперативното влијание на нарушувањето на безбедноста или губењето на интегритетот на мрежите и услугите, како дополнителни секторски показатели се земаат предвид следните прагови:

нарушувањето трае повеќе од еден час, а процентот на засегнати корисници е поголем од 15 % од вкупниот број корисници на операторот;

нарушувањето трае повеќе од два часа, а процентот на засегнати корисници е поголем од 10 % од вкупниот број корисници на операторот;

нарушувањето трае повеќе од четири часа, а процентот на засегнати корисници е поголем од 5 % од вкупниот број корисници на операторот;

нарушувањето трае повеќе од шест часа, а процентот на засегнати корисници е поголем од 2 % од вкупниот број корисници на операторот или

нарушувањето трае повеќе од осум часа, а процентот на засегнати корисници е поголем од 1 % од вкупниот број корисници на операторот.

(2) Операторот го пријавува и секое нарушување со кое е оневозможено остварување повик кон Единствениот европски број за итни повици „112“ или кон друг број за пристап до служба за итни повици.

(3) Праговите од ставот (1) на овој член се применуваат заедно со критериумите и праговите утврдени со прописите со кои се уредува безбедноста на мрежни и информациски системи и не ги заменуваат тие критериуми и прагови.

Член 11

Праговите од член 10 од овој правилник се однесуваат посебно на секоја од следните услуги:

- 1) фиксна телефонија;
- 2) мобилна телефонија;
- 3) фиксен интернет и
- 4) мобилен интернет.

Член 12

При известувањето за настанато нарушување на безбедноста или губење на интегритетот на мрежите или услугите од член 7 од овој правилник, операторот ги доставува информациите содржани во образецот од Прилог 1, кој е составен дел на овој правилник, во онаа фаза на известувањето во која тие му се достапни.

IV. ИЗВЕСТУВАЊА ЗА НАРУШУВАЊЕ НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ

1. Известување до Агенцијата за електронски комуникации и Агенцијата за заштита на личните податоци

Член 13

(1) Во случај на нарушување на безбедноста на личните податоци, операторот на јавни електронски комуникациски услуги е должен веднаш, но не подоцна од 24 часа од моментот на утврдување на нарушувањето, да достави известување до Агенцијата за електронски комуникации и до Агенцијата за заштита на личните податоци.

(2) Известувањето од ставот (1) на овој член се доставува по електронски пат, преку безбедните канали за известување објавени од Агенцијата за електронски комуникации и од Агенцијата за заштита на личните податоци и се потпишува од одговорното лице на операторот на начин утврден за користениот канал.

(3) Известувањето ги содржи информациите од Прилог 2, кој е составен дел на овој правилник, а особено опис на последиците од нарушувањето и предложените или преземените мерки за негово отстранување.

(4) Се смета дека операторот го утврдил нарушувањето во моментот кога стекнал доволно сознанија дека настанал безбедносен инцидент што довел до случајно или незаконско уништување, губење, промена, неовластено откривање или пристап до личните податоци на корисникот или на друго физичко лице.

(5) Доколку во рокот од ставот (1) на овој член не се достапни сите информации и се потребни понатамошни истражувања, операторот доставува иницијално известување со информациите од првиот дел на Прилог 2.

(6) Операторот доставува второ известување со информациите од вториот дел на Прилог 2 веднаш штом тие ќе станат достапни, но не подоцна од три дена по иницијалното известување. Ако во тој рок не може да ги обезбеди сите информации, операторот ги доставува информациите со кои располага и разумно го образложува доцнењето, а преостанатите информации и потребните измени ги доставува веднаш штом ќе станат достапни.

2. Известување до корисникот или друго физичко лице

Член 14

(1) Ако нарушувањето на безбедноста на личните податоци може негативно да влијае врз личните податоци или приватноста на корисникот или на друго физичко лице, операторот, покрај известувањето од член 13 од овој правилник е должен веднаш, но не подоцна од 24 часа од моментот на утврдување на нарушувањето да го извести засегнатиот корисник или физичкото лице.

(2) За утврдувањето на нарушувањето од ставот (1) на овој член се применува член 13 став (4) од овој правилник.

(3) При процената на можните негативни влијанија операторот особено ги зема предвид следните околности:

- 1) природата и содржината на засегнатите лични податоци, особено финансиските податоци, податоците за локација, записите за користење интернет, историјата на веб-прелистување, податоците за електронски пораки, деталните сметки за повици и посебните категории лични податоци;
- 2) можните последици за корисникот или физичкото лице, вклучувајќи злоупотреба на идентитет, измама, физичка штета, психолошка болка, понижување или штета на угледот и

3) околностите под кои настанало нарушувањето, особено кражба на податоците или сознание дека податоците неовластено ги поседува трето лице.

(4) Околностите од ставот (3) на овој член се индикативни насоки. Нивното непостоење не го ослободува операторот од обврската за известување ако постои реална можност за негативно влијание врз личните податоци или приватноста на корисникот или на друго физичко лице.

(5) Известувањето ги содржи информациите од Прилог 3, кој е составен дел на овој правилник, а особено природата на нарушувањето, точките за контакт каде што може да се добијат повеќе информации и препорачаните мерки за ублажување на можните негативни влијанија.

(6) Известувањето треба да биде изразено на јасен и лесно разбирлив јазик и не смее да се користи за промовирање или рекламирање нови или дополнителни услуги.

(7) Операторот го доставува известувањето преку комуникација што обезбедува брз прием и соодветна безбедност. Информациите се однесуваат само на нарушувањето на безбедноста на личните податоци.

(8) Доколку операторот што има директен договорен однос со крајните корисници во рокот од ставот (1) на овој член не може успешно да ги идентификува сите засегнати физички лица, известувањето го објавува преку национален или регионален медиум во истиот рок и продолжува со сите разумни напори за идентификување и поединечно известување на засегнатите лица.

3. Технички мерки за заштита

Член 15

(1) Операторот не мора да го извести корисникот или другото физичко лице согласно член 14 од овој правилник само доколку по добиеното известување од член 13 од овој правилник, Агенцијата за електронски комуникации донесе мислење со кое ќе утврди дека операторот за личните податоци на кои се однесува нарушувањето имплементирал соодветни технички мерки со кои податоците се направени неразбирливи за секое лице што нема право на пристап до нив.

(2) Агенцијата за електронски комуникации го доставува мислењето од ставот (1) на овој член до операторот и до Агенцијата за заштита на личните податоци.

(3) Податоците се сметаат за неразбирливи за лице што нема право на пристап, особено ако:

- 1) се безбедно криптирани со стандарден алгоритам, клучевите за декриптирање не се компромитирани и се генерирани и заштитени на начин што спречува неовластено дознавање со расположливи технички средства или
- 2) се заменети со хеширана вредност генерирана со стандардна криптографска функција со клуч, при што клучот не е компромитиран и е генериран и заштитен на начин што спречува неовластено дознавање со расположливи технички средства.

Член 16

Агенцијата за заштита на личните податоци, независно од мислењето од член 15 од овој правилник, може да бара од операторот за одредено нарушување на безбедноста на личните податоци да го извести корисникот или другото физичко лице, земајќи ги предвид можните негативни ефекти од нарушувањето.

4. Користење на друг оператор

Член 17

Доколку електронската комуникациска услуга се обезбедува преку друг оператор што нема директен договорен однос со крајниот корисник, тој оператор е должен веднаш по

утврдувањето на нарушувањето на безбедноста на личните податоци, да го извести операторот што има директен договорен однос со крајниот корисник.

V. ПРОВЕРКА НА МЕРКИТЕ ШТО ОПЕРАТОРИТЕ ГИ ПРЕЗЕМААТ ЗА ОБЕЗБЕДУВАЊЕ НА БЕЗБЕДНОСТ И ИНТЕГРИТЕТ НА ЈАВНИТЕ ЕЛЕКТРОНСКИ КОМУНИКАЦИСКИ МРЕЖИ И УСЛУГИ

Член 18

(1) Агенцијата за електронски комуникации може да изврши проверка на мерките што операторите ги преземаат за обезбедување на безбедноста и интегритетот на јавните електронски комуникациски мрежи и услуги и од операторите да побара:

- 1) да ѝ ги достават потребните информации за проценка на безбедноста и/или интегритетот на нивните мрежи и услуги, вклучувајќи ја усвоената политика за безбедност и
- 2) да обезбедат безбедносна ревизија што ја врши квалификувано независно тело или надлежен државен орган и резултатите да ѝ ги стават на располагање на Агенцијата за електронски комуникации.

(2) Безбедносната ревизија од ставот (1) точка 2) на овој член се спроведува во случаите, под условите и на начин утврдени со прописите со кои се уредува безбедноста на мрежни и информациски системи. Трошоците за ревизијата се поднесуваат согласно со тие прописи.

Член 19

(1) Агенцијата за електронски комуникации врши надзор над исполнувањето на обврските на операторите за обезбедување на безбедноста и интегритетот на јавните електронски комуникациски мрежи и услуги, согласно Законот за електронските комуникации и овој правилник.

(2) Во рамките на надзорот, Агенцијата може да ги испита случаите на неусогласеност, да го оцени нивното влијание врз безбедноста и интегритетот на мрежите и услугите и да побара доставување на податоци, документи и докази потребни за утврдување на фактичката состојба.

(3) Кога случајот опфаќа прашања од надлежност на друг орган, Агенцијата соработува со тој орган, при што настојува да се избегне повторно барање на исти податоци и документи од операторот.

VI. РЕГИСТАР НА НАРУШУВАЊА НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 20

(1) Операторите на јавни електронски комуникациски услуги се должни да водат регистар на нарушувања на безбедноста на личните податоци.

(2) Регистарот за секое нарушување ги содржи:

- 1) фактите и причините за нарушувањето на безбедноста на личните податоци;
- 2) последиците предизвикани од нарушувањето;
- 3) преземените мерки за безбедност на личните податоци и
- 4) другите информации од Прилозите 2 и 3 што им овозможуваат на Агенцијата за електронски комуникации и на Агенцијата за заштита на личните податоци да ја проверат усогласеноста на операторот со член 197 од Законот за електронските комуникации и со овој правилник.

(3) Регистарот се води во електронска форма, хронолошки, на начин што обезбедува точност, целосност, доверливост и достапност на внесените податоци и се става на **располагање на Агенцијата за електронски комуникации и на Агенцијата за заштита на личните податоци по нивно барање.**

VII. ЗАВРШНИ ОДРЕДБИ

Член 21

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

(2) Со денот на влегувањето во сила на овој правилник престанува да важи Правилникот за обезбедување на безбедност и интегритет на јавните електронски комуникациски мрежи и услуги и активностите што операторите треба да ги преземат при нарушување на безбедноста на личните податоци („Службен весник на Република Македонија“ бр. 9/15 и „Службен весник на Република Северна Македонија“ бр. 92/19).

(3) По влегувањето во сила, овој правилник се објавува и на веб-страниците на Агенцијата за електронски комуникации и на Агенцијата за заштита на личните податоци.

Бр: _____

29.09.2026 година, Скопје

**Агенција за
електронски комуникации**

Директор

Nusret Haliti

**Агенција за
заштита на личните податоци**

Директор,

Nakil Fetai

Прилог 1

Образец за известување на компјутерски инциденти

Датум на инцидентот

Година

Засегнат сервис

Фиксна телефонија

Траење (часови)

Број на корисници

Фиксен интернет

Траење (часови)

број на корисници

Мобилна телефонија

Траење (часови)

број на корисници

Мобилен интернет

Траење (часови)

број на корисници

Засегната технологија

PSTN

DSL

Fibre

Cable

GSM

UMTS

LTE

Друго

Основна причина за инцидентот

Системска грешка

Човечка грешка

Компјутерски напад

Природна непогода/невреме

Грешки од трета страна

Информација дали при настанувањето на инцидентот се засегнати сервисите на итните служби:

Иницијална причина:

(Пример: пресечен кабел, софтверска грешка, снабдување со струја, физички напад, поплава, грешка во следење на процедура, преоптеретување, лошо одржување)

Последователна причина:

(Пример: пресечен кабел, софтверска грешка, снабдување со струја, физички напад, поплава, грешка во следење на процедура, преоптеретување, лошо одржување)

Засегната опрема:

(Пример: свичеви, базни станици и контролери, трансмисиона мрежа, интерконекција, систем за ладење)

Опис

Научени лекции

Прилог 2

Содржина на известувањето за нарушувањето на безбедноста на личните податоци што операторот го доставува до националните регулаторни тела

Прв дел

Идентификација на операторот

Име на операторот

Контакт податоци (име и презиме, електронска пошта и телефонски број) за овластеното лице за заштита на личните податоци (офицер за заштита на личните податоци) или друго лице кај кое што може да се добијат повеќе податоци

Прво известување (да/не)

Второ известување (да/не)

Почетни информации во однос на нарушувањето на безбедноста на личните податоци

Датум и време на инцидентот (доколку се знае; во спротивно може да се направи проценка)

Датум и време на детектирање на инцидентот

Околности под кои што е настанато нарушувањето на безбедноста на личните податоци (пример: загуба, кражба, копирање)

Природа и содржина на засегнатите лични податоци

Применети технички и организациони мерки (или што ќе се применат) од операторот во однос на засегнатите лични податоци

Релевантна инволвираност на други оператори (доколку е применливо)

Втор дел

Дополнителни информации во однос на нарушувањето на безбедноста на личните податоци

Сумарен преглед на нарушувањето на безбедноста на личните податоци (вклучително физичка локација и медиум на кој се складирали податоците)

Број на корисници или физички лица што се засегнати

Потенцијални последици и негативни ефекти на корисникот или физичкото лице

Технички и организациони мерки преземени од операторот со цел да ги намали потенцијалните негативни ефекти

Известување до корисникот или физичкото лице што ја има направено операторот

Содржина на известувањето

Комуникациска технологија преку која е испратено известувањето

Број на корисници или физички лица кои што се известени

Прилог 3

Содржина на известувањето за нарушувањето на безбедноста на личните податоци што операторот го доставува до корисникот или физичкото лице

Име на операторот

Контакт податоци (име и презиме, електронска пошта и телефонски број) за овластеното лице за заштита на личните податоци (офицер за заштита на личните податоци) или друго лице кај кое што може да се добијат повеќе податоци

Причина поради која дошло до нарушување на безбедноста на личните податоци

Датум и време на инцидентот (доколку се знае; во спротивно може да се направи проценка)

Природа и содржина на засегнатите лични податоци (член 14, став 3 од Правилникот)

Можни последици од нарушувањето на безбедноста на личните податоци по корисникот или физичкото лице

Околности под кои што е настанато нарушувањето на безбедноста на личните податоци (пример: загуба, кражба, копирање)

Применети технички и организациони мерки (или што ќе се применат) од операторот во однос на засегнатите лични податоци

Мерки кои што операторот ги предлага на крајниот корисник со цел да се намалат негативните ефекти од овој инцидент.

Безбедносни мерки

Подрачја за преземање безбедносни мерки	Референтни Безбедносни мерки
Процедури за управување со генералните безбедносни ризици,	– Воспоставување и одржување на соодветни процедури за информациска сигурност која се однесува на мрежна сигурност како и на сигурност на услугите и личните податоци (Information security policy) – Воспоставување и одржување на соодветна рамка за управување со ризикот, која ќе послужи за идентификација и адресирање на ризикот (Governance and risk management) – Воспоставување и одржување на соодветна структура на улоги и одговорности (Security roles and responsibilities) – Воспоставување и одржување на соодветни процедури кои се однесуваат на договорите со трети страни и заштита за истите да не влијаат негативно на безбедноста на мрежите и услугите (Security of third party assets) .
Безбедност на човечките ресурси	– Проверка на персоналот (персонал , договорни страни и трети страни) кога е потребно согласни нивните задолженија и одговорности (Background checks); – Персоналот да се запознае со доволно информации за безбедност, а исто така да се обезбедат редовни обуки на тема безбедност (Security knowledge and training); – Воспоставување и одржување на соодветни процедури при кадровски промени и промени на улоги и одговорности кај (Personnel changes); – Воспоставување и одржување на соодветни процедури за персоналот кои ја прекршуваат политиката за безбедност како и воведување на дисциплински постапки (Handling violations);

Безбедност на системите и објектите,	– Воспоставување и одржување на соодветна физичка сигурност и сигурност на условите во објектите (Physical and environmental security of facilities); – Воспоставување и одржување на соодветна безбедност при снабдувањето (електрична енергија, гориво, или климатизација) за објектите (Security of supplies); – Воспоставување и одржување на соодветни (логички) контроли за пристап до мрежите и информациските системи, со цел да се спречи недозволен пристап, измена или бришење на податоците од таквите системи (Access control to network and information systems); – Воспоставување и одржување на интегритетот на мрежата и информацискиот систем, заштита од тројанци, “code injections” и друг малicioзен софтвер кој може да ја промени функционалноста на системите (Integrity of network and information systems); – Воспоставување и одржување на соодветни процедури за доверливост и интегритет на содржината на комуникациите и метаподатоците за комуникациите (Confidentiality of communications).
Безбедност на обработката на личните податоци	– Воспоставување и одржување на систем за заштита на личните податоци согласно прописите за заштита на личните податоци. – Планирање, воспоставување, применување, преиспитување и ажурирање на технички и организациски мерки за обезбедување на безбедност на обработката на личните податоци согласно прописите за заштита на личните податоци.
Безбедност и интегритет на личните податоци	- Воспоставување и одржување на систем за заштита на личните податоци согласно прописите за заштита на личните податоци - Применување на технички и организациски мерки за обезбедување на тајност и заштита на обработката на личните податоци согласно прописите за заштита на личните податоци
Оперативно управување	– Воспоставување и одржување на соодветни процедури за управување со критичните мрежни и информациски системи (Operational procedures); – Воспоставување на процедури за управување со критичните мрежни и информациски системи, со цел да се намалат инцидентите кои се предизвикани од промени (Change management); – Воспоставување и одржување на процедури за управување со средствата и контрола на

	конфигурацијата со цел управување со расположливите критични средства и конфигурација на критичните мрежни и информациски системи (Asset management).
Управување со инциденти	– Воспоставување и одржување на процедури за управување со безбедносните инциденти како и нивно проследување до одговорните лица (Incident management procedures); – Воспоставување и одржување на соодветни капацитети за детектирање на безбедносните инциденти (Incident detection capability); – Воспоставување и одржување на соодветни процедури за известување за безбедносните инциденти согласно законската регулатива (Incident reporting and communication);
Управување со деловниот континуитет	– Воспоставување и одржување на планови за вонредни ситуации и стратегија за обезбедување на континуитет на мрежи и услуги (Service continuity strategy and contingency plans); – Воспоставување и одржување на “disaster recovery” капацитети за повторно воспоставување на работа на мрежата и услугите во случај на природни катастрофи (Disaster recovery capabilities)
Мониторинг и тестирање на безбедносните мерки	– Воспоставување и одржување на системи за надзор на логовите на критичните мрежни и комуникациски системи (Monitoring and logging policies); – Воспоставување и одржување на процедури за тестирање на плановите за вонредни ситуации и креирање сигурносни копии, а кога е потребно и во соработка со трети страни (Exercise contingency plans); – Воспоставување и одржување на процедури за тестирање на мрежните и информациските системи, посебно при поврзување со нова мрежа или информациски систем (Network and information systems testing); – Воспоставување и одржување на соодветни процедури за извршување на проценка за безбедност и тестирање на мрежните и информатички системи (Security assessments); – Воспоставување и одржување на процедури за надзор и усогласеност со стандардите и законската регулатива (Compliance monitoring)

Прилог 5

Минимални безбедносни мерки	Референтни норми актуелна верзија на стандардот
Процедури за управување со генералните безбедносни ризици,	ISO/IEC 27001 ISO/IEC 27002 ISO/IEC 27005 ISO/IEC 27011
Безбедност на човечките ресурси,	ISO/IEC 27001 ISO/IEC 27002 ISO/IEC 27011
Безбедност на обработката на личните податоци	ISO/IEC 27001 ISO/IEC 27002 ISO/IEC 27005 ISO/IEC 27011 ISO/IEC 27701 ISO/IEC 29100
Безбедност на системите и објектите,	ISO/IEC 27001 ISO/IEC 27002 ISO/IEC 27011
Оперативно управување	ISO/IEC 27001 ISO/IEC 27002 ISO/IEC 27011
Управување со инциденти	ISO/IEC 27001 ISO/IEC 27002 ISO/IEC 27011
Управување со деловниот континуитет	ISO/IEC 22301 ISO/IEC 27011
Мониторинг и тестирање на безбедносните мерки	ISO/IEC 27001 ISO/IEC 27002 ISO/IEC 27011