201909201173

АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ

Врз основа на член 166 став (7) од Законот за електронските комуникации („Службен весник на Република Македонија“ бр. 39/14, 188/14, 44/15, 193/15, 11/18 и 21/18), директорот на Агенцијата за електронски комуникации во согласност со директорот на Дирекцијата за заштита на личните податоци, на 29 март 2019 година, донесе

ПРАВИЛНИК ЗА ИЗМЕНУВАЊЕ И ДОПОЛНУВАЊЕ НА ПРАВИЛНИКОТ ЗА ОБЕЗБЕДУВАЊЕ НА БЕЗБЕДНОСТ И ИНТЕГРИТЕТ НА ЈАВНИТЕ ЕЛЕКТРОНСКИ КОМУНИКАЦИСКИ МРЕЖИ И УСЛУГИ И АКТИВНОСТИ КОИ ШТО ОПЕРАТОРИТЕ ТРЕБА ДА ГИ ПРЕЗЕМАТ ПРИ НАРУШУВАЊЕ НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ*

Член 1

Во Правилникот за обезбедување на безбедност и интегритет на јавните електронски комуникациски мрежи и услуги и активности кои што операторите треба да ги преземат при нарушување на безбедноста на личните податоци („Службен весник на Република Македонија“ бр. 9/15), во членот 1 во алинејата 1 зборовите: „начинот на“ се заменуваат со зборовите: „начинот и роковите во“.

Во алинејата 2 зборовите: „начинот на доставување на известувањето на“ се заменуваат со зборовите: „ начинот и роковите на доставување на известувањето од“.

По алинејата 2 се додава нова алинеја 3 која гласи:

„-начинот и роковите на известување до Агенцијата за електронски комуникации од страна на операторите на јавни електронски комуникациски мрежи и услуги на годишно ниво,“.

Алинеите 3, 4 и 5 стануваат алинеи 4, 5 и 6.

Член 2

Во членот 2 се додава нова алинеја 1 која гласи:

„- Информациски систем: комуникациски, компјутерски или друг елекронски систем преку кој операторот ги обезбедува услугите согласно член 11 од овој правилник.“

Алинеите 1, 2 и 3 стануваат алинеи 2, 3 и 4.

Член 3

Во членот 4 се додава нова реченица која гласи:

„Со преземените чекори потребно е да се постигне одреден степен на сигурност кој ќе одговара на постоечките закани, ќе ги спречува безбедносните инциденти или ќе го ублажува влијанието на ваквите инциденти врз работата на јавните комуникациски мрежи и услуги.“

Член 4

Членот 6 се менува и гласи:

---

* Со овој правилник се врши усогласување со европската регулатива во областа на електронските комуникации, и тоа: одредбите од членот 13.а од Директивата 2002/21/ЕС које е донесесена од Европскиот парламент за обезбедување на заедничка рамка за регулација на електронските комуникациски мрежи и услуги и која е изменета и дополнета со Директивата 2009/140/ЕС и Регулативата на Комисијата (ЕУ) 611/2013 од 24 јуни 2013 за мерките кои се применуваат за известување при нарушување на безбедноста на личните податоци врз основа на Директивата 2002/58/ЕК на Европскиот парламент и на Советот за приватноста и електронските комуникации.

„Политиката за безбедност која што треба да ја усвојат операторите согласно член 5 на овој правилник треба да ги опфаќа минимум следните подрачја (Листа 1):

- Процедури за управување со генералните безбедносни ризици,
- Безбедност на човечките ресурси,
- Безбедност на системите и објектите,
- Безбедност и интегритет на личните податоци,
- Оперативно управување,
- Управување со инциденти,
- Управување со деловниот континуитет,
- Мониторинг и тестирање на безбедносните мерки.

Минималните безбедносни мерки кои треба да ги преземат операторите и кои треба да се содржани во Политиката за безбедност, како и референтните норми за нивно спроведување се наведени во Листата 2. Освен наведените референтни норми операторите можат да применат и други соодветни норми со цел остварување на безбедносните мерки наведени во ставот 1 на овој член.

Листите 1 и 2 од овој член се составен дел од овој правилник.“

Член 5

По членот 6 се додаваат два нови члена 6 - а и 6 - б кои гласат:

„Член 6 - а

Операторите кои се нотифицирани се должни да достават документирана Политика за безбедност пред започнување на давање на услугите од членот 11 на овој правилник.

Член 6 - б

Операторите се должни еднаш годишно да спроведат безбедносна проверка на информацискиот систем, со цел да се потврди дали се исполнети минималните пропишани мерки за безбедност наведени во Листата 2. Наодот од проверката, заедно со планот за отстранување на констатираните недостатоци, како и политиката за безбедност до колку е ревидирана, потребно е да се достават до Агенцијата за електронски комуникации до крајот на мај во тековната година, за претходната година. Постапката за безбедносната проверка може да ја реализира операторот или квалификувано независно тело кое врши безбедносна проверка.“

Член 6

Во членот 7 во последната реченица зборовите: „телото надлежно за справување со компјутерски инциденти во Република Македонија“ се заменуваат со зборовите: „ Националниот центар за одговор на компјутерски инциденти MKD-CIRT“.

Член 7

Во членот 10 се додава нов став 2 кој гласи:

„Операторите треба да ја известат Агенцијата доколку со нарушувањето е оневозможено остварување на повик кон итните служби со повикувачки броеви пропишани во Правилникот за единствениот европски број за итни повици „112“ („Службен весник на Република Македонија“ бр.184/15).“

Член 8

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

По влегувањето во сила, овој правилник ќе биде објавен и на веб-страницата на Агенцијата за електронски комуникации и Дирекцијата за заштита на личните податоци.

Агенција за електронски
комуникации
Директор,
Сашо Димитријоски, с.р.

Дирекција за заштита
на личните податоци
Директор,
Горан Трајковски, с.р.

Бр. 0201-1065/1
29 март 2019 година
Скопје

Листа 1

Безбедносни мерки

Подрачја за превземање 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 малциозен 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 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 сличај 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).

Листа 2

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 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