Врз основа на член 32 став (3) и член 33 став (2) од Законот за електронско управување („Службен весник на Република Македонија“ бр.105/09), министерот за информатичко општество донесе

ПРАВИЛНИК ЗА СТАНДАРДИТЕ И ПРАВИЛАТА ЗА БЕЗБЕДНОСТ НА ИНФОРМАЦИСКИТЕ СИСТЕМИ КОИ ШТО СЕ КОРИСТАТ ВО ОРГАНИТЕ ЗА КОМУНИКАЦИЈА ПО ЕЛЕКТРОНСКИ ПАТ

Член 1

Со овој правилник се пропишуваат за стандардите и правилата за безбедност на информациските системи кои што се користат во министерствата, другите органи на државната управа, организациите утврдени со закон и други државни органи, судовите, јавните обвинителства и државното правобранителство, правни и други лица на кои со закон им е доверено да вршат јавни овластувања, органите на општините, на градот Скопје и на општините на градот Скопје (во натамошниот текст: органи), за комуникација по електронски пат.

Член 2

Стандардите и правилата за безбедност на информациските системи опфаќаат:

- минимални критериуми и безбедносни мерки кои треба да ги исполнуваат информациските системи;
- минимални општи насоки за заштита на информациите од намерни и ненамерни неавторизирани промени, уништување или откривање;
- користење на безбедносните стандарди од серијата МКС ISO/IEC 27000 во информациските системи;
- редовна проверка на безбедноста на информациските системи;
- редовна проценка на ризиците поврзани со безбедноста на информациските системи, нивен приоритет, како и мерки за справување со ризиците во случај на нивна појава;
- надлежност и одговорност за воведување, управување и надзор на безбедноста на информациските системи.

Член 3

При остварување на административни услуги по електронски пат од страна на органите се:

- овозможува услови за воведување на политики, стандарди, начела, насоки, упатства или прирачници, потребни за ефективна функционалност и подобрување на безбедноста на информациските системи;
- следат потребите за подобрување на безбедноста на информацискиот систем согласно редовната проценка на информациските ризици и плановите за нивно управување и се обезбедуваат услови (финансиски, кадровски, технички, програмски) за нивна реализација;
- преземаат мерки и активности за функционирање на безбедноста на информацискиот систем и реализација на планираните подобрувања на истиот;
- дава согласност и се обезбедуваат услови за спроведување на редовна годишна проверка на безбедноста на информацискиот систем согласно прописите за електронско управување;
- спроведуваат препораките кои произлегуваат од заклучоците од редовната годишна проверка;
- обезбедува потребно оспособување и континуирана надградба на потребните знаења на кадарот за ефективно спроведување на безбедноста на информацискиот систем.

Член 4

За спроведување на безбедност на информациските системи од страна на органите при размена на податоци и документи во електронска форма, односно остварување на административни услуги по електронски пат, треба да се:

- донесат и применат политика за управување со информациска безбедност и интерни акти за нејзино спроведување;
- воспостават безбедносни мерки согласно проценетиот ризик од потенцијалните информациски закани;
- воспостават безбедносни мерки со кои ќе обезбеди доверливост, интегритет и достапност на информациите;
- воспостават безбедносни технички и организациски мерки за:
- заштита на личните податоци,
- редовна проценка на ризиците и ажурирање на плановите за справување со приоритетните ризици и воспоставување на евиденција на ризици,
- редовна или случајна проверка на безбедноста на информациските системи со изготвување на извештај со наоди и препораки;

- воспостават механизми за утврдување на сопственост на информациите и информациските средства;
- воспостават механизми за справување со безбедносни инциденти;
- утврдат и воспостават нивоа на доверливост на информациите и нивоа на пристап до нив;
- применуваат двојна контрола и поделба на работните задачи поврзани со двојната контрола;
- воспостават правила за „чист екран" и „чиста маса";
- воспостават процедури и правила за чување на записи.

Член 5

Одговорното лице за информациска безбедност на информациските системи определено во органите, при размена на податоци и документи во електронска форма, односно остварување на административни услуги по електронски пат:

- врши координација на сите безбедносни активности во однос на воспоставување и одржување на информациска безбедност;
- управува со периодичните проценки на ризиците за информацискатa безбедност;
- врши редовна проценка на ризиците и ажурирање на плановите за справување со приоритетните ризици;
- ја ажурира евиденцијата на закани и потенцијални ризици;
- го координира спроведувањето на безбедносни контроли и ја набљудува нивната ефикасност;
- предлага политика и упатства за постигнување на безбеден информациски систем;
- учествува во подготвувањето на интерните акти, технички и дополнителни комплементарни политики со кои се обезбедува спроведување на политиката и упатствата за безбеден информациски систем;
- го надгледува спроведувањето на интерните акти за безбедност на информацискиот систем;
- врши внатрешна координација и истрага на настаните што ја загрозиле безбедноста на информацискиот систем, вклучувајќи и соработка со надворешни органи и други институции;
- предлага мерки за надминување на последиците и спречување на слични инциденти;
- го известува функционерот кој раководи со органот со цел преземање координирана акција за заштита на органот од можни материјални и нематеријални загуби;

- соработува со одговорните лица за безбедност на информациските системи на надворешни органи и други институции;
- соработува со одговорното лице за заштита на лични податоци во органот, како и со одговорните лица за заштита на лични податоци од надворешни органи и други институции;
- работи на подигање на свеста за информацискатa безбедност;
- поднесува барање за покренување на постапка за утврдување на одговорност за повреда на правила за безбедност на информацискиот систем.

Член 6

Редовни интерни проверки за функционирањето, ефектите и слабостите во безбедноста на информацискиот систем се вршат од страна на органите.

За извршените редовни интерни проверки од ставот 1 на овој член се изготвуваат извештаи кои се достапни за увид на Министерството за информатичко општество.

Проверки во смисла на член 37 од Законот за електронско управување на функционирањето, ефектите и слабостите во безбедноста на информацискиот систем на органите, се вршат најмалку еднаш годишно од страна на Министерството за информатичко општество.

За спроведената проверка од ставот 3 на овој член се изготвува извештај со препораки за подобрување на безбедноста на информацискиот систем кој се доставува до органот.

Од страна на органот се врши надворешна контрола на безбедноста на информацискиот систем, најмалку еднаш во три години.

Надворешната контрола од ставот 5 на овој член се врши од страна на независно трето правно лице од областа за која што се врши контролата, определено од органот.

Извештајот од надворешната контрола од ставот 5 на овој член треба да биде достапен за увид на Министерството за информатичко општество.

Член 7

Содржината и минималните барања за безбедност на информациските системи во органите треба да бидат според следните стандарди:

- МКС ISO/IEC 27000 - Информациска технологија -- Безбедносни техники -- Систем за управување со информациска безбедност -- Преглед и речник;
- МКС ISO/IEC 27001 - Информациска технологија -- Безбедносни техники – Системи за управување со безбедност на информации - Барања;
- МКС ISO/IEC 27002 - Информациска технологија -- Безбедносни техники -- Начела за управување со безбедност на информации.

Член 8

Дејствијата по оценка и управување на ризикот, следењето и управувањето на инциденти поврзани со информациска безбедност и нивоата на доверливост на информациите и нивоа на пристап до нив, органите ги спроведуваат согласно насоките донесени од страна на Министерството за информатичко општество.

Член 9

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

Бр.11-745
18 јуни 2010 година
Скопје

Министер,
м-р Иво Ивановски