20192634115

МИНИСТЕРСТВО ЗА ИНФОРМАТИЧКО ОПШТЕСТВО И АДМИНИСТРАЦИЈА

Врз основа на член 34 ставови (2) и (3) и член 35 од Законот за електронско управување и електронски услуги („Службен весник на Република Северна Македонија“ бр. 98/19 и 244/19), министерот за информатичко општество и администрација донесе

ПРАВИЛНИК ЗА НАЧИНОТ И ПРОЦЕДУРАТА ЗА УПИС ВО ЛИСТАТА НА ПРАВНИ ЛИЦА КОИ ВРШАТ ПРОВЕРКА ЗА ИНТЕРОПЕРАБИЛНОСТ НА ИНФОРМАЦИСКИТЕ СИСТЕМИ, ФОРМАТА И СОДРЖИНАТА НА СЕРТИФИКАТИТЕ ЗА ИНТЕРОПЕРАБИЛНОСТ, ПРОЦЕДУРАТА ЗА ИЗДАВАЊЕ СЕРТИФИКАТ ЗА ИНТЕРОПЕРАБИЛНОСТ И ПРОЦЕДУРИТЕ ЗА ПРОВЕРКА НА БЕЗБЕДНОСТА И ИНТЕРОПЕРАБИЛНОСТА НА ИНФОРМАЦИСКИТЕ СИСТЕМИ

Член 1

Со овој правилник се пропишуваат начинот и процедурата за упис во листата на правни лица кои вршат проверка за интероперабилност на информациските системи, формата и содржината на сертификатите за интероперабилност, процедурата за издавање сертификат за интероперабилност и процедурите за проверка на безбедноста и интероперабилноста на информациските системи.

Член 2

Правните лица кои вршат дејност од областа на информациско-комуникациските технологии, односно проверка на системите за интероперабилност на информациски системи, треба:

- да се регистрирани за вршење на дејност или дополнителна дејност од областа на информациско-комуникациските технологии во Централниот регистар на Република Северна Македонија,
- да поседуваат важечки сертификати ISO 9001, ISO 20000 и ISO 27001,
- да поседуваат банкарска гаранција од 100.000 евра кон Министерството за информатичко општество и администрација (во натамошниот текст: Министерството),
- да поседуваат осигурување од општа одговорност во износ од 100.000 евра во денарска противвредност,
- да има вработено лице со валиден сертификат ISO/IEC 27001 Lead Auditor,
-во последните три години да има спроведено ревизија или усогласување со стандарди од областа на информациските системи во најмалку едно правно лице.

Член 3

Правните лица кои сакаат да бидат впишани во листата на правни лица кои вршат проверка за интероперабилност на информациските системи (во натамошниот текст: листата), поднесуваат барање за упис до Министерството.

Кон барањето за упис барателот ја приложува следната документација:

- тековна состојба издадена од Централен регистар на Република Северна Македонија не постара од шест месеци или од соодветен регистар доколку се работи за странско правно лице,
- заверена копија од сертификат ISO:9001,
- заверена копија од сертификат ISO:20000,
- заверена копија од сертификат ISO:27001,

- доказ за банкарска гаранција на износ од 100.000 евра кон Министерството за времето на траење на сертификатот,
- доказ за осигурување од општа одговорност до 100.000 евра во денарска противвредност кон Министерството за времето на траење на сертификатот,
- изјава заверена на нотар под материјална и кривична одговорност за доверлива препорачана испорака на документи и заштита на содржаните лични податоци,
- M1/M2 образец за лицето кое има валиден сертификат ISO/IEC 27001 Lead Auditor,
- заверена копија од сертификатот ISO/IEC 27001 Lead Auditor издадено за вработеното лице,
- копија од договорот согласно кој правното лице спровело ревизија или усогласување со стандарди од областа на информациските системи кај друго правно лице во последните три години.

Член 4

По приемот на барањето од член 3 од овој правилник, од страна на Министерството се утврдува исполнетоста на техничките барања најдоцна 30 дена од денот на приемот на барањето.

Ако правното лице ги исполнува техничките барања за упис од членот 2 од овој правилник, се внесува во листата од страна на Министерството согласно податоците кои правното лице ги навело во барањето за упис.

Правното лице кое е запишано во листата за целото времетраење додека е заведено во листата треба да ги исполнува техничките барања наведени во членот 2 од овој правилник.

Од страна на правното лице запишано во листата секоја година се докажува исполнетоста на техничките барања со доставување на целокупната документација наведена во член 3 став 2 од овој правилник до Министерството.

Ако правното лице престане да исполнува едно или повеќе од наведените техничките барања, се брише од листата од страна на Министерството.

Член 5

Правно лице кое во последните пет години извршило каква било имплементација или спровело усогласување со стандарди поврзана со информациски систем или дел од информациски систем во органот или другиот субјект кој бара проверка на системите за интероперабилност, не може да ја изврши таквата проверка во тој орган или друг субјект или да се јави како подизведувач.

Член 6

Правното лице кое е запишано во листата, а за кое од страна на Министерството е активирана банкарската гаранција, не може да врши проверка на интероперабилност на информациски системи во период од една година од денот на активирањето на банкарската гаранција.

Член 7

Процедурата за издавање сертификат за интероперабилност на информациски системи е:

- Сертификација за Ниво 1 (технички стандарди) за исполнување на техничките барања кои се дадени во Прилог бр. 1 кој е составен дел на овој правилник (во натамошниот текст: сертификат за Ниво 1) или
- Сертификација за Ниво 2 (организациски стандарди) за исполнување на техничките барања кои се дадени во Прилог бр. 2 кој е составен дел на овој правилник (во натамошниот текст: сертификат за Ниво 2).

Член 8

Сертификатите издадени за нивоата од членот 7 од овој правилник имаат важност од три години од денот на издавањето.

Спроведувањето на проверка на системите за интероперабилност на информациските системи за добивање на сертификат за Ниво 2 се врши од страна на органот или другиот субјект кој спровел проверка на системите за интероперабилност на информациските системи и добил сертификат за Ниво 1, најдоцна пет години, сметано од првото добивање на сертификат за Ниво 1.

Ако органот или другиот субјект кој спровел проверка на системите за интероперабилност на информациските системи и добил сертификат за Ниво 1, не успее согласно ставот 2 на овој член да добие сертификат за Ниво 2, од страна на Министерството по спроведена проценка на ризик, може да се ограничи или оневозможи пристапот на тој орган или субјект до националната платформа за интероперабилност – Македонска информациска магистрала (во натамошниот текст: МИМ).

Член 9

Сертификацијата за ниво 1 се врши од страна на Министерството по претходно поднесено барање за спроведување на проверка на системите за интероперабилност на информациските системи од страна на органот или другиот субјект.

Сертификација за ниво 2 врши правно лице регистрирано во листата, по претходно поднесено барање за спроведување на проверка на системите за интероперабилност на информациските системи од органот или другиот субјект, согласно Законот за јавните набавки.

Од страна на Министерството се врши проверка на информациските системи кои разменуваат податоци преку МИМ на начин што се проверува исполнувањето на секое техничко барање поединечно за ниво 1.

Од страна на правното лице се врши проверка на информациските системи кои разменуваат податоци преку МИМ на начин што се проверува исполнувањето на секое техничко барање поединечно за ниво 1 и за ниво 2.

Пред започнување со вршење на проверката, службеното лице од органот или другиот субјект и овластеното лице од правното лице потпишуваат изјава за взаемна доверливост на податоци.

Член 10

По извршувањето на проверката на системите за интероперабилност со МИМ, Министерството или правното лице кое ја извршило проверката на системите за интероперабилност на информациските системи, изготвува извештај за проверка на системите за интероперабилност на информациските системи.

Извештајот треба да содржи најмалку:

- докази за секоја контрола посебно,
- наоди за секоја контрола посебно,
- оценка на исполнетост за секоја контрола посебно,
- вкупна оценка и суштински наоди,
- препораки за подобрување групирани по приоритет врз база на тоа каква акција е потребна: како итни, важни и нормални.

Извештајот од ставот 1 на овој член се поднесува до органот или другиот субјект кај кого е извршена проверката најдоцна 15 дена од денот на извршената проверка.

По извршената проверката од страна на Министерството на органот или другиот субјект кој ја побарал проверката, му се издава сертификат за интероперабилност со МИМ, доколку ги исполнува сите технички барања за Ниво 1.

Од страна на правното лице кое ја извршило проверката се издава сертификат за интероперабилност со МИМ на органот или другиот субјект кој ја побарал проверката, доколку ги исполнува сите технички барања за Ниво 1 и Ниво 2.

Од страна на органот или другиот субјект кај кого е извршена проверката на системите за интероперабилност на информациските системи се испраќа копија од извештајот од ставот 1 на овој член до Министерството најдоцна 15 дена од денот на приемот на извештајот.

Член 11

Сертификатот за интероперабилност со МИМ се издава во хартиена и во електронска форма.

Сертификатот од ставот 1 на овој член содржи:

- лого на издавачот,
- назив на органот или другиот субјект кому му е издаден сертификатот,
- ниво на сертификација за интероперабилност,
- сериски број,
- датум на издавање,
- рок на важност и
- потпис од овластено лице и печат.

Образецот на сертификатот за интероперабилност со МИМ е даден во Прилог бр. 3 и е составен дел на овој правилник.

Член 12

Органот или другиот субјект кој има валиден сертификат за ISO/IEC 27001, а кој не е приклучен на МИМ и кој нема извршено проверка на системите за интероперабилност на информациските системи, се смета дека ги исполнува техничките барања за сертификација на ниво 2.

Органот или другиот субјект од ставот 1 на овој член, може да биде приклучен на МИМ за периодот за кој е определена валидноста на сертификатот, по поднесено барање за приклучување на МИМ со приложување на заверена копија од валидниот сертификат ISO/IEC 27001.

Член 13

Од страна на Министерството се врши проверка на интероперабилност на информациски системи за Ниво 1 најдоцна 45 дена од денот на приемот на барањето од член 9 став 1 од овој правилник.

Член 14

Со денот на влегувањето во сила на овој правилник престанува да важи Правилникот за начинот на сертифицирање на информациските системи кои ги користат органите за комуникација по електронски пат, како и за формата и содржината на сертификатот за функционалност на информациските системи („Службен весник на Република Македонија“ бр. 152/16).

Член 15

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

Бр. 08/1-3954/7
17 декември 2019 година
Скопје

Министер за информатичко
општество и администрација,
Дамјан Манчевски, с.р.

ПРИЛОГ БР. 1

ТЕХНИЧКИ БАРАЊА ЗА СЕРТИФИКАЦИЈА
на интероперабилност на информациски систем со МИМ ЗА НИВО 1

Сите пропишани технички барања за интероперабилност на информациски систем со МИМ за Ниво 1 се однесуваат на

- комуникацискиот клиент, и
- информацискиот систем којшто треба да разменува податоци преку МИМ.

За сертификација на Ниво 1 потребно е да биде исполнети следните технички барања, од кои барањата означени со (*) се задолжителни. Доколку некое од останатите технички барања не е исполнето, органот или другиот субјект треба да даде соодветно образложение.

1. Политики и процедури
   - усвоена Политика за информациска безбедност

2. Физички пристап и безбедност

2.1. Технички барања за сервер сала
- огноотпорна безбедносна врата;
- соодветна противпожарна заштита (интертен гас); *
- подигнат антистатички под;
- нема инсталации за вода и греење во сервер сала;
- сите прозори и врати се обезбедени; *
- соодветна климатизација; *
- соодветно напојување; *
- не се складира запалив материјал во сервер салата. *

2.2. Физички пристап до сервер сала
- салата е заклучена и пристапот е регулиран; *
- постои евиденција за лицата кои има пристап до систем салата;*
- видео надзор.

Напомена: доколку органот или другиот субјект не управува со сервер салата во која е сместена опремата, и доколку не е во можност да обезбеди физички пристап за да се изврши проверката, органот или другиот субјект треба да достави соодветен доказ дека овие технички барања се исполнети како договорна обврска.

3. Логички пристап и безбедност

3.1. Логичка шема на системот

- краток опис на информацискиот систем (име, цел, користени технологии, поврзаност со други системи);*
- мрежен дијаграм на високо ниво, на кој е претставен информацискиот систем којшто треба да разменува податоци преку МИМ, како и неговата поврзаност со комуникацискиот клиент.*

3.2. Назначени се лица на позициите:

- одговорно лице за безбедност на информациски системи;*
- мрежен администратор;
- системски администратор;
- администратор на база на податоци.

Напомена: На позициите наведени во последните три алинеи може да се назначени надворешни лица согласно важечки договор за одржување. Договорот или одредби на договорот за одржување кои ги содржат горенаведените барања треба да се направат достапни за увид.

3.3. Контрола на пристап

- политика на лозинки на ниво на оперативен систем и на ниво на апликација;*
- листа на корисници на апликацијата којашто разменува податоци преку МИМ и нивни привилегии.

4. Технички барања за размена на податоци и документи
   - Органот или другиот субјект е приклучен на владината оптичка мрежа или поседува активна интернет конекција преку која може да воспостави VPN

ПРИЛОГ БР. 2

ТЕХНИЧКИ БАРАЊА ЗА СЕРТИФИКАЦИЈА
на интероперабилност на информациски систем со МИМ ЗА НИВО 2

Доколку институцијата поседува валиден ISO/IEC 27001 сертификат, се смета дека ги исполнува техничките барања неопходни за сертификација на НИВО 2.
Наведените политики и други акти може да бидат составен дел од друг акт ако во тој акт се содржани сите потребни елементи.
За секое техничко барање, освен интерниот акт со кој е регулиран, треба да се провери и исполнувањето на истиот. Доколку некој од техничките барања не е исполнет, органот или другиот субјект треба да даде соодветно образложение.
За сертификација на Ниво 2 е потребно да се исполнат сите технички барања предвидени со НИВО 1, а дополнително и следните технички барања:

1. Управување со информациски средства, која опфаќа:
   - Попис на средства
   - Сопственост на средствата
   - Прифатлива употреба на средства
   - Враќање на средствата
   - Класификација на информации
   - Означување на информациите
   - Ракување со средства
   - Управување со преносни уреди
   - Отстранување на медиуми
   - Физички и електронски пренос на медиуми

2. Политика за контрола на пристап, која опфаќа:
   - Физичка заштита
   - Контрола на пристапот до мрежа и до мрежни сервиси
   - Регистрирање и одјавување на корисник
   - Управување со правата на пристап на корисниците
   - Тајност на информации за автентикација и управување со лозинки
   - Ревидирање на правата на пристап и привилегиите
   - Укинување или приспособување на правата на пристап
   - Ограничување на пристапот до информации
   - Постапки за безбедно најавување

- Истекување на времето на сесијата
- Политики за пристап од далечина

3. Политика за прифатлива употреба на системите, која опфаќа:
   - Сопственост на системите и средствата
   - Користење на електронска пошта
   - Неприфатлива употреба на системите и мрежата

4. Постапка за управување со промени, која опфаќа:
   - Лица одговорни за управување со промени
   - Барање за промена
   - Анализа на барање за промена
   - Класификација на промената
   - управување со системски закрпи на информациските системи

5. Физичка безбедност и безбедност на опкружувањето, која опфаќа:
   - Периметар на физичка безбедност и безбедносни зони
   - Контрола при физички влез
   - Заштита од закани од надворешното окружување
   - Работење во безбедносни зони
   - Безбедност на опремата
   - Одржување на опремата
   - Изнесување на средства и безбедност надвор од работните простории
   - Безбедно отстранување или повторна употреба на опремата

6. Методологија за процена на ризици, која опфаќа:
   - Назначување на тимот за процена на ризици
   - Избор на методологија за процена на ризици
   - Идентификување на ризиците
   - Изготвување на матрица на ризици
   - Справување со ризиците
   - Периодични преиспитувања

7. Политика за резервна копија на која опфаќа:
   - периодично креирање на резервна копија
   - периодично тестирање на враќање на податоците од резервната копија
   - начин на заштита, обележување и чување на медиумите за резервна копија

8. Процедура за Управување со инциденти по информацискиот систем, која опфаќа:
   - начин на пријавување на инциденти
   - класификација на инциденти
   - начин на одговор и справување со инцидентот
   - преземање мерки за во иднина тој инцидент да не се повтори
   - известување за инциденти

9. План за континуитет на деловни процеси и оporавување од катастрофи
   - Дефинирање на деловни процеси и нивни сопственици
   - Спроведување оценка на влијанието на испади по информацискиот систем на деловното работење (БИА) и приоритетизација на критичните деловни процеси
   - Преземање мерки за обезбедување континуитет на критичните деловни процеси
   - Редовно тестирање на планот за континуитет на деловни процеси и оporавување од катастрофи

10. Процедура за управување со записи (log management)
   - кои активности се запишуваат во лог датотеките
   - заштита на лог датотеките
   - период на чување
   - администраторски логови
   - обработка и следење на логови

11. Политика за заштита од вируси и друг злонамерен софтвер

ПРИЛОГ БР. 3

Место за лого на издавачот на сертификатот

Врз основа на член 34 став (1) од Законот за електронско управување и електронски услуги се издава:

СЕРТИФИКАТ

за интероперабилност на информациски систем на

_____

(назив на органот или другиот субјект)

За ниво _____на интероперабилност на системи со МИМ

Сериски бр._____

Датум на издавање_____

Важи до_____

(три години)

М. П

Потпис

_____