Врз основа на член 158-s точка 1 од Законот за супервизија на осигурување - пречистен текст („Службен весник на Република Македонија“ бр.30/2012), Одлука на Уставен суд бр.202/2011 („Службен весник на Република Македонија“ бр. 45/2012), Одлука на Уставен суд бр.130/2011 („Службен весник на Република Македонија“ бр.60/2012), Одлука на Уставен суд бр.122/2011 („Службен весник на Република Македонија“ бр. 64/2012) и Одлука на Уставен суд бр.129/2011 („Службен весник на Република Македонија“ бр. 23/2013), Советот на експерти на Агенцијата за супервизија на осигурување донесе

ПРАВИЛНИК ЗА МИНИМАЛНИТЕ СТАНДАРДИ НА ИНФОРМАЦИСКИТЕ СИСТЕМИ НА ДРУШТВАТА ЗА ОСИГУРУВАЊЕ

I. Општи одредби

Член 1

(1) Со овој правилник се пропишуваат минималните стандарди кои треба да бидат задоволени во работењето на информациските системи на друштвата за осигурување (во понатамошниот текст: друштвата).

(2) Пропишаните минимални стандарди од став (1) на овој член се однесуваат на управувањето, безбедноста и работењето на информациските системи на друштвата, како и обезбедување на континуитет на работење во случај на некој катастрофален настан.

II. Управување со информациските системи

Член 2

Друштвата се должни да воспостават адекватен информациски систем кој ги задоволува следните услови:

1. Поседува соодветни функционалности, капацитет и перформанси кои овозможуваат извршување на бизнис процесите;
2. Обезбедува навремени, точни и потполни информации кои се неопходни за секојдневното работење, како и донесување одлуки во друштвото и

3. Содржи соодветни контроли при внес на податоците, нивна обработка, како и при излез на обработените податоци, кои овозможуваат спречување или детекција на грешки или некозистентност во податоците или информациите.

Член 3

Друштвото е должно да го надгледува, ревидира и континуирано да го унапредува информацискиот систем, како и процесот на управувањето со истиот, со цел да се обезбеди адекватна функционалност на истиот согласно условите наведени во член 2 од овој правилник.

Член 4

Друштвото е должно да дефинира организациона структура каде јасно ќе бидат дефинирани задачите и одговорностите на сите вработени кои учествуваат во работењето, одржувањето и унапредувањето на информацискиот систем.

Член 5

Друштвото е должно да обезбеди примена на сите усвоени интерни акти и процедури во врска со информацискиот систем, како и да овозможи сите корисници на информацискиот систем да бидат информирани за содржината на овие акти и процедури во согласност со нивните овластувања, одговорности и потреби.

Член 6

(1) Друштвото е должно да донесе стратегија за развој на информацискиот систем, како засебен документ или во склоп на генаралната стратегија за развој, која ќе биде во согласност со потребите на работењето на Друштвото.

(2) Друштвото е должно оваа стратегија да ја ревидира и усогласува согласно промените во работењето на Друштвото.

Член 7

Друштвото е должно да изготви и пропише методологија со која ќе се дефинираат критериумите, начините и постапките за управување со проекти во врска со информацискиот систем.

III. Управување со ризици

Член 8

Друштвото е должно да воспостави процес на управување со ризиците на информацискиот систем кој ќе опфати идентификација и вреднување на ризиците, како и преземање мерки за нивно отстранување, ублажување или пренесување.

Член 9

Друштвото е должно да изготви и пропише методологија за анализа на ризиците на информацискиот систем и нивно вреднување т.е. евалуација. Методологијата треба јасно да го дефинира системот за определување на магнитудата на ризикот (анализа), како и процесот на споредување на ризиците согласно разни критериуми на веројатност на истиот, за да се определи значајноста на ризикот (евалуација).

Член 10

Друштвото треба да изготви и пропише соодветен документ „Регистар на ризици“ каде ќе се чуваат информациите за идентификуваните ризици, мерките кои се предложени и преземени за нивно отстранување, ублажување или пренесување.

Член 11

(1) Друштвото е должно да формира Одбор за ризици на информацискиот систем (во понатамошниот текст: Одбор за ризици) кој ќе ги врши активностите предвидени во процесот на управување со ризиците на информацискиот систем, т.е. ќе врши идентификација, анализа и евалуација на ризиците, ќе предлага мерки за нивно

отстранување, ублажување или пренесување, ќе го ажурира „Регистарот на ризици“ и ќе ја верификува имплементацијата на предложените мерки.

(2) Одборот за ризици треба да биде составен од најмалку два члена. Во Одборот за ризици на информацискиот систем задолжително членува и раководното лице задолжено за информацискиот систем.

(3) Доколку Друштвото има формирано одбор за ризици кој ги покрива сите ризици на работењето, истиот може да ги врши и функциите на Одбор за ризици на информацискиот систем доколку во овој одбор како член е вклучено и раководното лице задолжено за информацискиот систем.

Член 12

Одборот за ризици е должен редовно да врши анализа и евалуација на ризиците на информацискиот систем и да го ажурира „Регистарот на ризици“, и тоа најмалку двапати годишно.

Член 13

Одборот за ризици е должен во процесот на управување со ризиците да ги вклучи и сите нови проекти во врска со информацискиот систем уште од фазата на проектирање на истите.

Член 14

Одборот за ризици е должен да доставува извештај за својата работа, по секој од одржаните состаноци, до органот на управување на Друштвото. Извештајот треба да содржи и ажуриран регистар на ризици.

Член 15

Мерките за отстранување, ублажување или пренесување на ризиците предложени од Одборот за ризици, се имплементираат доколку бидат усвоени од органот на управување на Друштвото.

IV. Безбедност на информацискиот систем

Член 16

(1) Друштвото, во согласност со сложеноста на информацискиот сиситем, е должно да изготви и пропише политика за безбедност на информацискиот систем.

(2) Политиката за безбедност на информацискиот систем ги дефинира принципите, начините и процедурите кои се употребуваат за постигнување на адекватното ниво на безбедност, како и одговорностите и овластувањата на сите корисници во врска со безбедноста и ресурсите на информацискиот систем.

(3) Друштвото е должно редовно да ја ажурира политиката за безбедност на информацискиот систем согласно промените во опкружувањето и промените во самиот информациски систем.

Член 17

(1) Друштвото е должно да воспостави континуиран процес на управување со безбедноста на информацискиот систем. Овој процес треба да ги идентификува потенцијалните безбедносни недостатоци на информацискиот систем, да ги регистрира сите безбедносни инциденти и да имплементира контроли кои ќе ги отстранат овие безбедносни недостатоци и ќе обезбедат адекватно ниво на безбедност на информацискиот систем.

(2) Процесот на управување со безбедноста задожително треба да ги земе предвид и безбедносните ризици кои произлегуваат од процесот на управување со ризици.

Член 18

(1) Друштвото е должно да имплементира соодветни контроли за пристап до ресурсите на информацискиот систем, како и да имплементира адекватен систем за управување со правата на пристап на корисниците.

(2) Системот на управување со корисничките права треба да ги имплементира процесите за идентификација, авторизација и автентикација на корисниците, евиденција на корисниците и нивната активност во информацискиот систем, како и надзор над управувањето (доделување и одземање) на корисничките права.

(3) Доделувањето на кориснички права Друштвото е должно да го спроведува врз основа на принципот за давање на најмалку можни права на пристап потребни за непречено извршување на работните обврски.

(4) Друштвото е должно периодично или по потреба, а најмалку еднаш годишно, да врши проверка на корисничките права.

(5) Друштвото е должно да обезбеди повисоко ниво на безбедност на корисниците кои имаат надворешен пристап кон информацискиот систем, најмалку со имплементирање на енкриптирана конекција и автентикација со 2 фактора.

Член 19

(1) Друштвото е должно да воспостави и спроведува процес на креирање и чување на резервна копија на податоците на информацискиот систем.

(2) Друштвото е должно да изготви и пропише процедура за креирање и чување резервна копија на податоците на информацискиот систем, и тоа: податоците неопходни за деловно работење на Друштвото, записите од системот за управување со корисничките права, како и резервна копија на самите апликации т.е. нивните инсталациски датотеки кои се користат како дел од информацискиот систем.

(3) Процедурата за креирање и чување резервна копија треба детално да ги опише ресурсите за кои се изготвува ваква копија, начините на кои се врши истото, фреквенцијата на изготвување на овие копии, како и времетраењето и местото на кое се чуваат.

(4) Друштвото е должно да води евиденција за креираните копии и да врши периодично тестирање на медиумите на кои се чуваат резервните копии, како и тестирање на процесот на враќање на податоците од резервната копија најмалку еднаш годишно.

(5) Резервните копии кои се чуваат надвор од просториите на Друштвото задолжително треба да бидат енкриптирани.

V. Управување со деловен континуитет

Член 20

Друштвото е должно да воспостави процес на управување со деловниот континуитет со цел да обезбеди непречено и континуирано функционирање на сите критични системи и процеси, како и да ги ограничи губитоците во услови на вонредно работење.

Член 21

(1) Друштвото е должно да управува со деловниот континуитет врз основа на изработена анализа на влијанијата на работењето и на процена на ризиците, која треба да опфати:

1. Дефинирање на критичните деловни процеси неопходни за непречено и континуирано функционирање на Друштвото;
2. Дефинирање на ресурсите и системите потребни за извршување на поединечните деловни процеси, како и нивните меѓусебни зависности и врски;
3. Процена на ризикот за секој од поединечните деловни процеси, како и веројатноста за настан на несакани случувања и нивното влијание на континуитетот на работењето, финансиските загуби и репутацијата на Друштвото;
4. Дефинирање на нивото на прифатливи ризици и техниките за ублажување на идентификуваните ризици;
5. Дефинирање на најдолгиот прифатлив прекин на работењето за секој од процесите.

(2) Врз основа на изработената анализа, Друштвото е должно да усвои стратегија за деловен континуитет, која ќе го дефинира следното:

1. Приоритетите на враќање во функција на деловните процеси, како и потребните ресурси и системи за таа намена;
2. Нивоа на потребен капацитет на деловните процеси (SDO);
3. Неопходно време на враќање за деловните процеси (RTO) и
4. Дефинирање на точка на враќање на деловните процеси (RPO).

(3) Стратегијата за деловен континуитет се усвојува од органот на управување на Друштвото.

Член 22

(1) Друштвото е должно, врз основа на усвоената стратегија за деловен континуитет од член 21, да изготви и усвои план за деловен континуитет кој ќе содржи:

1. Опис на процедурите во случај на престанок на работењето, вклучително и начинот на стапување на планот во сила;
2. Листа на идентификуваните критични процеси согласно стратегијата за деловен континуитет, како и нивните SDO, RTO и RPO;
3. Ажурирана листа на ресурсите потребни за воспоставување на континуитет на работењето;
4. Ажурирани контакт податоци за лицата кои учествуваат во реализацијата на планот за континуитет, како и нивните задачи и одговорности.
5. Соодветни процедури за повторно воспоставување на информациските системи кои се неопходни за поддршка на деловните процеси предвидени со планот за деловен континуитет.

(2) Планот за деловен континуитет се усвојува од органот на управување на Друштвото.

Член 23

Друштвото е должно да изготви соодвени процедури за повторно воспоставување на информациските системи кои се неопходни за поддршка на деловните процеси предвидени со планот за деловен континуитет. Овие процедури се дел од планот за континуитет и истите треба да содржат:

1. Листа на неопходни ресуси потребни за повторно воспоставување на информацискиот систем или соодветниот потсистем;
2. Листа на лицата кои ќе учествуваат во повторното воспоставување на информацискиот систем или соодветниот потсистем, со нивните задачи и обврски;
3. Процедура/упатство за повторно воспоставување на информацискиот систем или соодветниот потсистем со детален опис на сите чекори потребни за враќање на оперативноста на истиот.

Член 24

Друштвото е должно периодично или по потреба, а најмалку еднаш во две години, да ги ажурира и ревидира анализата, стратегијата и планот за деловен континуитет.

Член 25

(1) Друштвото е должно периодично или по потреба, а најмалку еднаш во две години, да го тестира планот за континуитет. Тестирањето да биде изведено на начин на кој ќе се верификува функционалноста на планот во реални услови.

(2) Друштвото е должно да изготви записник од тестирањето на планот за континуитет и да изврши соодветни корекции на планот согласно забележаните недостатоци.

(3) Записниците од тестирањето на планот за континуитет на работењето се усвојуваат од органот на управување на Друштвото.

Член 26

Друштвото е должно редовно да ги информира сите лица учесници во планот за деловен континуитет за содржината и промените во истиот, согласно нивните задачи и одговорности во имплементацијата на планот.

VI. Управување со надворешни добавувачи на услуги за информациски технологии

Член 27

(1) Друштвото е должно да воспостави процес на управување со услугите од надворешните добавувачи на услуги за информациски технологии (во понатамошниот текст: ИТ услуги). Целта на овој процес е да се воспостават соодветни процедури за одлучување при изборот на добавувачот, управување на нивото на сервис, како и исполнување на договореното ниво од страна на добавувачот.

(2) Услугите, како што се набавка и одржување на ИТ опрема, телекомуникациски услуги и набавка на готов софтвер кој е комерцијално достапен на пазарот (off-the-shelf), не се предмет на овој процес.

Член 28

Друштвото е должно да изготви и усвои процедура за одлучување за избор на добавувач на ИТ услуги со која задолжително ќе предвиди:

1. Анализа на потенцијалните добавувачи на ИТ услуги во однос на нивните технички способности за давање на бараната услуга, финансиската состојба на добавувачот и неговата деловна репутација;
2. Доколку добавувачот е од друга држава или држави, да утврди дали прописите на тие држави дозволуваат соодветна контрола на работењето на добавувачот од страна на Агенцијата за супервизија на осигурување за ИТ услугите кои ги испорачува кон Друштвото и
3. Анализа на потешкотиите и времето потребно за избор на друг добавувач, или можностите за извршување на истите услуги во самото Друштво, во случај на престанок на давање на услугата од страна на добавувачот.

Член 29

Друштвото е должно да изготви и усвои процедура за управување со нивото на сервис на добавувачот на ИТ услуги, при што задолжително ќе предвиди:

1. Уредување на правата за лиценцирање, сопственоста на изворниот код, како и правата на интелектуална сопственост;
2. Уредување на правата за преземање на правата на изворниот код во случаи каде добавувачот не е во можност на ја испорача услугата (escrow arrangement);
3. Уредување на правата за увид и контрола на работењето на добавувачот на ИТ услугите за конкретната услуга која е предмет на договорот со Друштвото;
4. Уредување на параметрите на нивото на сервис;
5. Уредување на начинот за известување за остварeното ниво на сервис и
6. Уредување на проверката и следењето на усогласеноста со законските прописи на добавувачот на ИТ услугите.

Член 30

Договорите кои Друштвото ги склучува со добавувачот на ИТ услуги, а кои меѓу другото предвидуваат и обработка, чување или пристап до податоците на Друштвото, задолжително треба да ги содржат и следните елементи:

1. Одредби за јасно разграничување на правата и обврските помеѓу Друштвото и добавувачот на ИТ услугата;

2. Одредби за дефинирање на можностите за предвремено раскинување на договорните обврски;

3. Одредби за усогласеност на добавувачот со соодветните законски прописи;

4. Одредба за тајност на податоците;

5. Одредби со кои на Друштвото му се овозможува непречен пристап и можност за контрола на просториите и податоците на добавувачот, во врска со услугите кои ги врши во име на институцијата.

Преку договорот Друштвото обезбедува непречен пристап и можност за контрола на просториите и податоците на надворешното лице и за АСО, како и за друштвото за ревизија кое врши ревизија на годишните финансиски извештаи на институцијата.

Притоа пристапот се однесува исклучиво на податоците кои се однесуваат на услугите кои надворешното лице ги врши за Друштвото.

VII. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Овој правилник влегува во сила со денот на објавување во „Службен весник на Република Македонија“” а ќе се применува од 1 јануари 2015 година.

Бр. 0201-1258/9 **Претседател на Советот на експерти**

19.12.2013 година **д-р Климе Попоски**

Скопје