**НАРОДНА БАНКА НА РЕПУБЛИКА МАКЕДОНИЈА**

Врз основа на член 47 став 1 точка 6 од Законот за Народната банка на Република Македонија („Службен весник на Република Македонија" бр. 158/10, 123/12 и 43/14), член 68 став 1 точка 5 и член 172 став 2 од Законот за банките („Службен весник на Република Македонија" бр. 67/07, 90/09, 67/10, 26/13 и 15/15), Советот на Народната банка на Република Македонија донесе

# ОДЛУКА
# за сигурноста на информативниот систем на штедилница
# („Службен весник на Република Македонија" бр. 74/15)

## I. ОПШТИ ОДРЕДБИ

1. Со оваа одлука се пропишува методологијата за сигурноста на информативниот систем на штедилница со која се воспоставуваат стандарди за сигурноста на информативните системи, преку дефинирање критериуми за воспоставување процес за управување со сигурноста на информативниот систем и за обезбедување непрекинатост во работењето.

2. Одделни изрази употребени во оваа одлука го имаат следново значење:

2.1. **Ризик од неадекватност на информативните системи (ИТ ризик)** е ризикот од загуба за штедилницата поради губење, неовластено користење или нерасположливост на информациите, информативните средства и/или услугите што ги нуди.

2.2. **Сигурноста на информативниот систем** на штедилницата се дефинира како исполнување на следниве критериуми:

- Доверливост: информативниот систем е достапен само за корисниците кои имаат овластен пристап до него;
- Интегритет: заштита на точноста и комплетноста на информативниот систем;
- Расположливост: непречен пристап до информативниот систем за овластените корисници.

2.3. **Тежок прекин на деловните процеси** претставува состојба во која штедилницата не е способна да ги исполни преземените деловни обврски поради причини коишто не може да ги контролира, или во случаи кога штедилницата е физички или телекомуникациски недостапна, односно не се достапни информациите и информативните системи на кои се одвиваат критичните операции на штедилницата.

2.4. **Сигурносен инцидент** е секој непланиран или непредвиден настан којшто може да ја наруши или да ги загрози сигурноста и функционалноста на информативните системи коишто ги поддржуваат деловните процеси на штедилницата.

2.5. Под **процена на ризикот** се подразбира воспоставување постојан процес којшто опфаќа:

- идентификација и класификација на средствата на информативниот систем на штедилницата;
- анализа на веројатноста за појавата на закани и слабости на информативниот системот и идентификација на можните последици;
- доделување приоритет на ризиците во зависност од големината на потенцијалната загубата што може да ја предизвикаат за штедилницата.

За извршената процена на ризикот од потточка 2.5 од ова точка, штедилницата треба да изработи извештај. Овој извештај се ажурира при значајни измени во информативниот систем.

## II. ПРОЦЕС НА УПРАВУВАЊЕ СО СИГУРНОСТА НА ИНФОРМАТИВНИОТ СИСТЕМ

3. Заради управување со ризикот од неадекватност на информативните системи, штедилницата е должна да воспостави процес за управување со сигурноста на информативниот систем којшто одговара на природата, обемот и сложеноста на финансиските активности што ги врши.

Процесот за управување со сигурноста на информативниот систем од ставот 1 од оваа точка опфаќа:

- процена на ризикот;
- политика за сигурност на информативниот систем;
- спроведување сигурносни контроли;
- тестирање на сигурноста;
- следење и надградба.

4. Штедилницата е должна да донесе и да примени политика за сигурност на информативниот систем со која се дефинираат основите на процесот за управување со сигурноста на информативниот систем.

Политиката од ставот 1 од оваа точка треба да ги содржи најмалку следниве елементи:

- стратегија за управување со идентификуваните ризици, преку воспоставување акциски план за обезбедување на сигурноста на информативниот систем;
- годишен план за обука на вработените, за правилно користење на услугите коишто се достапни преку информативниот систем на штедилницата;
- управување со сигурносните инциденти и воспоставување соодветен механизам за нивното идентификување, пријавување и ефикасно отстранување на можните закани за сигурноста на информативниот систем;
- дефинирање на улогата на лицето надлежно за работа на информатичката технологија од точка 8 од оваа одлука и интерни процедури за работа, во согласност со усвоените акти од областа

на управување со информатичката технологија и информативната сигурност;
- дефинирање на улогата на внатрешната и надворешната ревизија од аспект на обезбедување сигурност на информативниот систем и нејзино тестирање;
- систем за управување на пристапот на крајните корисници на системот, којшто опфаќа процес на евидентирање, идентификација, следење на корисничките права на пристап, особено на администраторскиот и далечинскиот пристап до ресурсите на информативниот систем,
- дефинирање на начинот на управување со измените во информативниот систем и управување со сигурносните надградби,
- дефинирање на начинот на воспоставување на планот за непрекинатост во извршувањето на деловните активности од точка 10 од оваа одлука;
- начин на воспоставување антивирусна заштита;
- дефинирање на начинот на телекомуникациско поврзување и обезбедување заштита на податоците коишто се трансферираат;
- дефинирање сигурносни зони преку кои ќе се ограничи физичкиот пристап до информациите и информативните средства;
- дефинирање на начинот на воспоставување дополнителни безбедносни механизми, како што се противпожарна заштита, заштита од поплава, системи за надзор, сензори и аларми;
- заштита на личните податоци, во согласност со важечките прописи во Република Македонија; и
- дефинирање на начинот на користење услуги од надворешни лица за софтвер и хардвер и следење на нивниот квалитет.

За ефикасна примена на политиката, односно на елементите на политиката дефинирани во ставот 2 од оваа точка, штедилницата е должна да воспостави соодветни процедури.

5. Политиката од точка 4 од оваа одлука содржи опис на административните, техничките и физичките сигурносни контроли и начинот на нивната примена во штедилницата.

Сигурносните контроли од ставот 1 од оваа точка треба да одговараат на големината и сложеноста на штедилницата, како и на видот на финансиските активности што ги врши.

6. Штедилницата е должна да воспостави процес на професионално, независно и објективно тестирање на ефикасноста и на соодветноста на спроведените сигурносни контроли содржани во политиката од точка 4 од оваа одлука.

7. Штедилницата треба да ги дефинира критериумите, начинот и постапките на информирање на органите на управување, за информациите поврзани со функционирањето и сигурноста на информативниот систем.

8. Штедилницата треба да именува лице коешто ќе биде одговорно за управување со информатичката технологија и да ги дефинира неговите одговорности и делокруг на работа.

9. Штедилницата треба да воспостави процес на управување со сигурносните инциденти којшто ќе овозможи навремен и ефикасен одговор во случај на нарушување на сигурноста и функционалноста на информативниот систем.

Во случај на сигурносен инцидент од највисок степен, штедилницата е должна да ја извести Народната банка за настанатиот инцидент, неговото влијание и преземените активности.

Штедилницата е должна да го достави известувањето од ставот 2 од оваа точка до Народната банка, во рок од 3 (три) дена од денот на настанување на сигурносниот инцидент.

## III. ПЛАН ЗА НЕПРЕКИНАТОСТ ВО РАБОТЕЊЕТО

10. Штедилницата е должна да развива и да спроведува сопствен план за непрекинатост во работењето, којшто ќе се темели врз повеќе сценарија и ќе овозможи оперативност и минимизирање на загубите во случај на тежок прекин на деловните процеси.

Планот од ставот 1 од оваа точка треба да ги содржи најмалку следниве елементи:

- идентификација на критичните операции, вклучувајќи ги и оние коишто зависат од надворешни лица;
- идентификација на алтернативните механизми за континуитет во деловните процеси во случај на прекин на примарните механизми;
- идентификација на можноста за обнова на податоците коишто се потребни за продолжување на деловниот процес;
- предвидување резервна локација на која ќе се одвиваат критичните деловни операции и на која ќе се чуваат заштитени копии од податоците. Локацијата треба да биде на соодветна оддалеченост од примарната, со цел да се минимизира ризикот двете локации да бидат истовремено недостапни.

За ефикасна примена на планот од ставот 1 од оваа точка, штедилницата е должна да воспостави процедури преку кои соодветно ќе се применат елементите дефинирани во став 2 од оваа точка.

11. Штедилницата треба да врши периодично тестирање и ажурирање на планот од точка 10 од оваа одлука.

## IV. ЗАВРШНИ ОДРЕДБИ

12. Оваа одлука влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Македонија", а ќе почне да се применува од 1

јануари 2016 година. Одредбите од главата III ќе почнат да се применуваат од 1 јануари 2017 година.

**О. бр. 02-15/IV - 4/2015**
**30 април 2015 година**
**Скопје**

**Гувернер**
**и претседавач**
**на Советот на Народната банка**
**на Република Македонија**
**Димитар Богов**