ОБЩИНА ИВАНОВО

УТВЪРЖДАВАМ

ГЕОРГИ МИЛАНОВ – КМЕТ НА ОБЩИНА ИВАНОВО

МЕТОДИКА ЗА АНАЛИЗ И ОЦЕНКА НА РИСКА ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ НА ОБЩИНА ИВАНОВО, ОБЛАСТ РУСЕ

СЛИЦЕ КЪМ ХОРАТА

2020 година

Раздел I

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата процедура е разработена на основание чл.7, ал.1-4 от НАРЕДБА за минималните изисквания за мрежова и информационна сигурност и е утвърдена със Заповед на Кмета на общината № РД-09-139/31.03.2020 г.

Чл. 2. По своята същност управлението на риска представлява съвкупност от процеси за идентифициране на потенциалните заплахи към носителите на информация и активите, участващи в предоставянето на електронни услуги, анализ и оценка на рисковете, породени от тези заплахи.

Чл. 3. Целта на процеса за управление на риска е да се минимизират загубите от потенциални нежелани събития, настъпили в резултат от реализиране на заплахи към сигурността на мрежите и информационните системи, които биха засегнали конфиденциалността, интегритета и достъпността на информацията, създавана, обработвана, предавана и унищожавана чрез тях.

Чл. 4. Процедурата има за цел да даде общ подход при анализа и оценката на риска за сигурността на информационните и комуникационните системи, предоставяни от различните администрации, с цел получаване на съизмерими, относително обективни и повтарящи се резултати чрез:

1. регламентиране на дейностите и тяхната последователност при анализа и оценката на риска за електронните услуги;
2. определяне на критериите;
3. определяне на приоритетите на риска.

Чл. 5. Оценката на риска се извършва по методика, гарантираща съизмерими, относително обективни и повтарящи се резултати.

Чл. 6. Настоящият документ се преглежда за адекватност минимум веднъж годишно, като при необходимост се актуализира или когато се налагат съществени изменения в целите, вътрешните и външните условия на работа, информационната и комуникационната инфраструктура, дейностите или процесите.

Раздел II

ТЕРМИНИ И ДЕФИНИЦИИ

Чл. 7. При изготвяне на анализ и оценка на риска за сигурността на информационните и комуникационните системи, използваните термини имат следното значение:

1. **Информационна сигурност** – запазване на цялостност, наличност и поверителност;
2. **Цялостност** – информацията и активите да са цели, пълни и с вярно съдържание;
3. **Наличност** – информацията и активите да са достъпни и използваеми;
4. **Поверителност** – предоставяне на информация и активи само на оторизирани служители и лица;
5. **Риск** – ефект на неопределеност. Възможността дадена заплаха да използва дадена уязвимост на актив и по този начин да причини вреда на организацията

6. **Остатъчен риск** - рискът, който остава след въздействието върху първоначално оценения риск.
7. **Заплаха** – потенциална причина за нежелан инцидент, който може да навреди на система или организация
8. **Вероятност** – възможността дадена заплаха да се осъществи
9. **Третиране на риска** – третиране на въздействие, уязвимост, вероятност
10. **Третиране на степента на заплаха / въздействие** – внедряване на мерки и контроли за намаляване на ефекта от заплахата върху актива (при реализирана заплаха);
11. **Третиране на вероятността** - внедряване на мерки и контроли, които оказват влияние върху външната(околната) среда на актива;
12. **Информационен актив** – информация свързана с дейността на организацията, носителите на тази информация, средствата за обработка на информацията, физическото място в което се обработва и съхранява;
13. **Отговорник на актива** – служител, който работи с него, съхранява или му е зачислен персонално;
14. **Собственик на риска** – служител, който взема решения за управлението и приемането на риска;
15. **Собственик на процес** – служител който отговаря за бизнес процес;

Раздел III

ИДЕНТИФИКАЦИЯ НА ЗАПЛАХИТЕ

Чл. 8. Вземайки под внимание външните и вътрешни фактори, които биха повлияли на дейността на Общинската администрация, всеки Директор на дирекция и началник на отдел определя и описва потенциалните заплахи, свързани с информационната сигурност в отделен прозорец на Риск-регистъра (електронна таблица).

Чл. 9. Поддържа се списък с примерни заплахи в Риск-регистъра.

Чл. 10. Всеки директор на дирекция и началник на отдел е собственик на риска, свързан с дейностите в неговото структурно звено и използваните от него активи.

Чл. 11. Собствениците на рискове описват в Риск-регистъра всички приложени мерки за защита имащи отношение към съответните заплахи.

Раздел IV

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

Чл. 12. Собственикът на риска определя въздействието по скалата и документира оценката в Риск-регистъра.

Стойност	Материални и нематериални щети, които заплахата ще причини, ако се реализира
5	Катастрофални щети свързани с репутация, финанси и отпадане на всички услуги

4	Големи щети свързани с репутация, финанси и отпадане на голяма част от услугите
3	Значителни щети свързани с финанси и отпадане на част от услугите
2	Малки щети свързани с финанси и затруднено използване на услугите
1	Незначителни щети свързани със затруднено използване на услугите

Раздел V

ОЦЕНКА НА ВЕРОЯТНОСТТА

Чл. 13. Собственикът на риска определя вероятността по скалата и документира оценката в Риск-регистъра.

Стойност	Честота
5	Реализирането на заплахата в рамките на 1 година е над 70%
4	Реализирането на заплахата в рамките на 1 година е от 50% до 70%
3	Реализирането на заплахата в рамките на 1 година е от 30% до 50%
2	Реализирането на заплахата в рамките на 1 година е от 10% до 30%
1	Реализирането на заплахата в рамките на 1 година е под 10%

Раздел VI

ОЦЕНКА НА РИСКА. ПРИОРИТЕТ.

Чл. 14. Собствениците на рискове оценяват риска в Риск-регистъра по формулата:

Риск = Въздействие x Вероятност.

Чл. 15. След оценката на риска приоритизирането на риска се разделя на три нива, като приемливото ниво е до 6.

ПРИОРИТЕТИ	ВЕРОЯТНОСТ				
ВЪЗДЕЙСТВИЕ	1	2	3	4	5
	2	4	6	8	10
	3	6	9	12	15
	4	8	12	16	20
	5	10	15	20	25

1. Рисковете в диапазона 1 - 6 се определят като приемливи, с **ПРИОРИТЕТ 3** и не се изисква да се предприемат мерки за намаляване на риска.
2. Рисковете в диапазона 8 – 12 се определят с **ПРИОРИТЕТ 2** и се прави анализ на възможните мерки, които биха могли да се предприемат за смекчаването им, и се преценява дали разходът на ресурси за прилагането им е пропорционален на щетите от реализиране на заплахата. В случай че щетите са повече от разходите, се определят отговорно лице и срок за прилагане на тези мерки.

3. Рисковете в диапазона 15 – 25 се приемат с **ПРИОРИТЕТ 1** и затова незабавно се планират мерки, които биха намалили риска от реализиране на конкретната заплаха, и се определят отговорници и срокове за прилагането им.

Раздел VII

НАМАЛЯВАНЕ НА РИСКА

Чл. 16. Рисковете с Приоритет 1 и по преценка с Приоритет 2 се включват в Риск-регистъра, където собствениците на рисковете планират нови мерки за намаляване на риска, определят съответните ресурси и срокове за внедряване им, след което оценяват остатъчния риск по гореописаната формула, отчитайки на кой от двата компонента (вероятност и въздействие) ще повлияе за намаляване.

Чл. 17. Остатъчните рискове се приемат от Кмета на Общинската администрация, като становището се документира със заповед.