



РЕПУБЛИКА БЪЛГАРИЯ

Министерство на околната среда и водите

РЕГИОНАЛНА ИНСПЕКЦИЯ ПО ОКОЛНАТА СРЕДА И ВОДИТЕ – РУСЕ

ЗАПОВЕД

№ 290.....

Русе, 15.06......2023 г.

На основание чл. 6, ал. 1, т.1 и т. 5 от Правилника за устройството и дейността на РИОСВ (ДВ, бр. 54 от 16.06.2020 г.), чл. 4 и чл. 5 от Наредбата за минималните изисквания за мрежова и информационна сигурност - НМИМИС (обн. ДВ, бр. 59 от 26.07.2019 г.)

НАРЕЖДАМ:

1. Утвърждавам:
 - 1.1. Политика по мрежова и информационна сигурност ;
 - 1.2. Вътрешни правила за управление на инциденти с мрежовата и информационна сигурност в РИОСВ-Русе;
 - 1.3. Правила за управление на физическата сигурност на информационните активи и сигурност на заобикалящата среда на РИОСВ-Русе;
 - 1.4. Методика за анализ и оценка на риска за сигурността на информационните и комуникационните системи на РИОСВ-Русе;
2. Политиката по мрежова и информационна сигурност да се публикува на страницата на РИОСВ-Русе в Интернет.
3. Електронно, чрез системата за електронен обмен, документите по т. 1 да се доведат до знанието на всички служители за сведение и изпълнение.

Контрол по изпълнение на заповедта възлагам на директор дирекция „АФПД“.

инж. I
Директ





РЕПУБЛИКА БЪЛГАРИЯ

Министерство на околната среда и водите

РЕГИОНАЛНА ИНСПЕКЦИЯ ПО ОКОЛНАТА СРЕДА И ВОДИТЕ – РУСЕ

УТВЪРЖДАЕ

инж. ЦОНКА

ДИРЕКТОР И



Версия	1.0
Дата	15.06.2023 г.
Класификация	TLP- WHITE

ПОЛИТИКА

ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

ПРЕДНАЗНАЧЕНИЕ

Документът е предназначен да изрази официално намеренията и насоките за управление на информационната сигурност в Регионалната инспекция по околната среда и водите – Русе.

С Политиката по мрежова и информационна сигурност РИОСВ – Русе цели да се приобщи към основните принципи и ценности, описани в Наредба за минималните изисквания за мрежова и информационна сигурност (ДВ, бр. 59 от 26.07.2019 г.).

- Осведоменост

Персоналът, клиентите на РИОСВ-Русе, доставчиците, подизпълнителите и всички останали участници в обмена на информация следва да са наясно с необходимостта от сигурност на информационните системи и мрежи и да допринасят за нейното повишаване.

- Отговорност

Всички участници в информационния обмен са отговорни за сигурността на информационните системи и мрежи.

- Реакция

Всички участници в информационния обмен трябва да действат своевременно и да си сътрудничат за предотвратяване, разкриване и реагиране на инциденти по сигурността.

- Оценка на риска

Рисковете за информационната сигурност следва да бъдат анализирани и оценявани.

- Управление на сигурността

Сигурността следва да бъде постигана чрез прилагането на цялостен подход за управление.

- Преоценка

Сигурността на информационните системи и мрежи следва да бъде преразглеждана и преоценявана минимум веднъж годишно, като при необходимост бъдат внасяни изменения в Политиката, процедурите, практиките и мерките.

Реализирането на тази Политика е от особена важност за осигуряване на висока надеждност при предоставяне на информационни услуги.

С Политиката по мрежова и информационна сигурност РИОСВ-Русе цели да постигне:

- защита на информацията от неразрешен достъп;
- запазване поверителността на информацията;
- недопускане разкриване на информация на неоправомощени лица;
- запазване на информацията от нерегламентирани промени;
- предоставяне на информацията на оправомощените лица винаги, когато е необходимо;
- спазване на нормативната уредба;
- обучение по информационната сигурност на всички участници в информационния обмен;
- документиране и проучване на всяко съмнение за нарушаване на информационната сигурност.

ПРИЛОЖИМОСТ

С тази Политика РИОСВ-Русе изразява своята решимост за въвеждане на цялостна система за предпазване на информацията и свързаните с нея активи от всякакви заплахи, както външни така и вътрешни, независимо от това дали са нарочни или неволни.

Целият персонал на РИОСВ-Русе е отговорен за прилагането на тази Политика в ежедневната си работа.

Ръководството на РИОСВ – Русе се ангажира с осигуряване необходимите ресурси и подпомагане усилията на всеки участник в информационния обмен за постигането на тази Политика.

1. ОСНОВНИ НАПРАВЛЕНИЯ

Основните направления на информационната сигурност, в които тази Политика ще търси реализация са:

- предпазване на информацията;
- предпазване на личните данни;
- осигуряване на доверие сред всички заинтересовани страни за надеждността на управляваната информация.

1.1. Стратегически и оперативни цели за мрежова и информационна сигурност

Подходът и дейностите за постигане на целта са свързани с:

- Усъвършенстване на информационната и технологична среда в РИОСВ-Русе;
- Осигуряване на висока защита на качеството на информацията и интегритета на данните;
- Осигуряване на резервираност и непрекъсваемост в процесите на информационния обмен.

2. ОТГОВОРНОСТИ

Ръководството на РИОСВ – Русе реализира тази Политика чрез въвеждане и прилагане на необходимите правила, процедури, инструкции, заповеди и други вътрешни актове на РИОСВ-Русе.

Пълномощията и отговорностите на ръководството на РИОСВ-Русе, насочени към осигуряване и поддържане на информационната сигурност в съответствие с изискванията на приложимите законови и други нормативни актове са регламентирани в съответните процедури и включват:

- Служител по мрежова и информационна сигурност - отговаря всички служители и други заинтересовани лица да бъдат напълно информирани по отношение на задълженията и отговорностите, включени в процедурите и инструкциите за информационна сигурност. Организира провеждането на периодичните проверки за сигурност на системите. Докладва на ръководството за състоянието на информационната сигурност в организацията.

- Директори на дирекции - носят отговорност по отношение на данните и другите информационни ресурси, използвани при дейностите, които се осъществяват под тяхното наблюдение и контрол, за да се гарантира, че те са адекватно защитени, а също така се спазват приложимите указания, процедури и механизми при изпълнението на съответните дейности.
- Служител, отговорен за системно администриране – отговаря за инсталацията, конфигурацията и администрирането на инфраструктурата, отговаря за ежедневната работа на информационните системи, като извършват процедури по архивиране, създаване на резервни копия на информация и възстановяване на информационните системи.
- Всички служители - служителите, вкл. временно наетите, посетителите, доставчици и подизпълнители, са длъжни да спазват указанията, процедурите и механизмите за информационна сигурност и активно да участват в опазването на информационните активи/ресурси. Те не трябва да имат достъп и да боравят с информационните активи без да имат съответните пълномощия и са длъжни да докладват на отговорните лица при установяване на нарушения по отношение на сигурността.

Всички участници в информационния обмен са длъжни:

- да спазват правилата, указани в документацията във връзка с мрежовата и информационна сигурност и другите вътрешни актове на РИОСВ-Русе;
- да съдействат с личен принос за осъществяването на тази Политика;
- да докладват за наблюдавани слабости в информационната сигурност.

3. ПОЛИТИКА ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

В РИОСВ – Русе са утвърдени и се прилагат Вътрешни правила за мрежова и информационна сигурност, които указват отговорностите и задълженията на служителите като потребители на информационните и комуникационните системи/ използване на персонални компютри, достъп до ресурсите на компютърната /корпоративната/ мрежа, генериране и съхранение на пароли, достъп до интернет, работа с електронна поща, системи за документооборот и други вътрешноведомствени системи/.

За осъществяването на тази Политика са разработени и се прилагат следните регламенти относно:

3.1 Оценка на риска

Оценката на риска се прилага към цялата информационна система и включва приложения, сървъри, компютърна мрежа и всеки процес или процедура, чрез които системата се администрира и/или поддържа. Във ведомството е разработена и утвърдена Методика за анализ и оценка на риска.

3.2 Управление на физическата сигурност на информационните активи

В РИОСВ – Русе са разработени и въведени Правила за управление на физическата сигурност на информационните активи.

3.3 Управление на инциденти и подобряване на мрежовата и информационната сигурност

С цел намаляване на риска и произтичащите от появата на инциденти разходи, Ведомството е разработило и внедрило Вътрешни правила за управление на инциденти с мрежовата и информационна сигурност.