РЕПУБЛИКА БЪЛГАРИЯ
Министерство на земеделието
Областна дирекция "Земеделие" - Хасково

З А П О В Е Д

№ РД-04-60
Хасково, 30.05.2023 **г.**

На основание чл.3, ал.3, т.1 и ал.4 от Устройствения правилник на Областните дирекции „Земеделие" и чл.6, ал.1, във връзка с чл.5. ал.1, т.6 и т.7 от Наредбата за минималните изисквания за мрежова и информационна сигурност

Н А Р Е Ж Д А М :

1. Утвърждавам Политика за мрежова и информационна сигурност в Областна дирекция „Земеделие" – Хасково.

2. Политиката по т.1 е неразделна част от Системите за финансово управление и контрол в Областна дирекция „Земеделие" – Хасково и следва да бъде публикувана на интернет страницата на Областна дирекция „Земеделие" – Хасково.

Настоящата заповед да се сведе до знанието на съответните длъжностни лица за сведение и изпълнение.

ВАЛЕНТИНА ДЕЛЧЕВА
Директор на ОД „Земеделие" - Хасково

РЕПУБЛИКА БЪЛГАРИЯ
Министерство на земеделието
Областна дирекция "Земеделие" - Хасково

УТВЪРДИЛ:

/ВАЛЕНТИНА ДЕЛЧЕВА/
Директор на ОД „Земеделие" - Хасково

П О Л И Т И К А

ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

В ОД „ЗЕМЕДЕЛИЕ" - ХАСКОВО

ХАСКОВО

2023 год.

Раздел I

Общи положения

Чл. 1. Политиката за мрежова и информационна сигурност има за цел да определи принципите на управление на мрежовата и информационна сигурност в Областна дирекция „Земеделие“ – гр. Хасково (ОДЗ).

Чл. 2. Политиката взема под внимание конкретните цели на държавната администрация за мрежова и информационна сигурност в контекста на общите стратегическите цели на ОДЗ за:

Стратегическа цел 1: „Трансформиране на администрацията и публичните институции в цифрови“

Специфична цел 1.1. Осигуряване на оперативна съвместимост на информационните ресурси по подразбиране

Специфична цел 1.2. Осигуряване на надеждност и мрежова и информационна сигурност на информационните ресурси на е-управление

Специфична цел 1.3. Осигуряване на цифрови решения, информационни системи и споделени ресурси на електронното управление

Специфична цел 1.4. Оптимизация на работните процеси в администрацията и промяна на модела на данни за предоставяне на електронни услуги по подразбиране (Digital by default)

Стратегическа цел 2: „Електронно административно обслужване, ориентирано към потребителя“

Специфична цел 2.1. Улесняване на взаимодействието и изграждане на доверие между потребителя и администрациите, публичните институции, лица, осъществяващи публични функции и организации, предоставящи обществени услуги.

Конкретни мерки, чрез които се постигат специфичните цели на ОДЗ:

1. Модернизация на комуникационната инфраструктура на ОДЗ:

1.1. Доставка, инсталация и конфигурация на комуникационно оборудване;

1.2. Изграждане на комуникационна свързаност на ОДЗ и Общинските служби по земеделие (ОСЗ);

2. Осигуряване на надеждност и мрежова и информационна сигурност на информационните ресурси на е-управление;

3. Модернизация и управление на информационната инфраструктура на ОДЗ:

3.1. Доставка и внедряване на ИТ компоненти;

3.2. Доставка на сървъри и сторидж;

3.3. Изграждане на виртуална сървърна среда и миграция на съществуващи инфраструктурни услуги;

3.4. Доставка на система за архивиране на информация;

3.5. Изграждане на регистри за информационни проекти и ресурси;

3.6. Разработване на вътрешноведомствена инструкция за реда и правилата на доставка, изграждане, поддържане, управление и наблюдение на информационни системи в ОДЗ;

4. Интегриране и централизиране на информацията:

4.1. Интегриране на системи/ регистри от специализираната администрация;

4.2. Интегриране на системи/ регистри от общата администрация;

5. Действия за подобряване на информационната сигурност в ОДЗ:

5.1. Система за предотвратяване изтичането на конфиденциална информация в ОДЗ;

5.2. Прилагане на изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)(ОВ L 119, 4.5.2016 г.) и Закона за защита на личните данни;

6. Развитие на електронните административни услуги предлагани от ОДЗ:

6.1. Анализ на съществуващата нормативна уредба и стратегически документи за интегриране на електронни административни услуги;

6.2. Определяне на административните услуги, които следва да се електронизират и включат в системата RegiX;

Чл. 3. За постигането на стратегическите цели, ОДЗ определя и внедрява мерки за мрежовата и информационната сигурност и подхода за постигането им в съответствие с нормативните актове и вътрешните правила.

Чл. 4. Настоящата политиката включва и специфични политики и процедури за мрежова и информационна сигурност в ОДЗ.

Чл. 5. Политиката има отношение към всички служители и външни лица (партньори, доставчици по договор, служители от други административни органи) на ОДЗ.

Чл. 6. При неспазване на настоящата политиката за мрежова и информационна сигурност ръководството на ОДЗ прилага законосъобразните мерки.

Раздел II

Принципи на управление на мрежовата и информационна сигурност

Чл. 7. За управлението и упражняването на контрол свързан със сигурността на информацията в ОДЗ, Директорът определя служители от ОДЗ, на които възлага дейности по мрежова и информационна сигурност, както следва:

1. да организират и контролират дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност, и целите, заложени в настоящата политика;
2. да участват в изготвянето на политиките и документираната информация;
3. да следят за спазването на Вътрешните правила и прилагането на законите, подзаконовите нормативни актове, стандартите, политиките и правилата за мрежовата и информационната сигурност;
4. да консултират ръководството на ОДЗ във връзка с информационната сигурност;

5. да ръководят периодичните оценки на рисковете за мрежовата и информационната сигурност;

6. периодично (не по-малко от веднъж в годината) да изготвят доклади за състоянието на мрежовата и информационната сигурност в ОДЗ и да ги представят на Директора;

7. да координират обученията, свързани с мрежовата и информационната сигурност;

8. да организират проверки за актуалността на плановете за справяне с инцидентите и плановете за действия в случай на аварии, природни бедствия или други форсмажорни обстоятелства. Да анализират резултатите от тях и организират изменение на плановете, ако е необкодимо;

9. да поддържат връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност;

10. да следят за правилното водене на Регистъра на инцидентите;

11. да уведомяват за инциденти съответния секторен екип за реагиране на инциденти с компютърната сигурност;

12. да организират анализ на инцидентите с мрежовата и информационната сигурност за откриване на причините за тях и предприемане на мерки за отстраняването им с цел намаляване на еднотипните инциденти и намаляване на загубите от тях;

13. да следят за актуализиране на използвания софтуер и фърмуер;

14. да следят за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлагат адекватни мерки за противодействието им;

15. да организират тестове за откриване на уязвимости в информационните и комуникационните системи и предлагат мерки за отстраняването им;

16. да организират и сътрудничат при провеждането на одити, проверки и анкети и при изпращането на резултатите от тях на съответния национален компетентен орган;

Чл. 8. За поддържането и развитието на мрежовата и информационна сигурност в ОДЗ, в съответствие с нормативните изисквания, се приемат и внедряват комплекс от организационни, технологични и технически мерки.

Чл. 9. Ръководството на ОДЗ осигурява необходимите ресурси за прилагане на пропорционални и адекватни на рисковете организационни, технически и технологични мерки, гарантиращи високо ниво на мрежова и информационна сигурност в обхвата на Наредбата.

Чл. 10. (1) В ОДЗ се разработват и внедряват Вътрешни правила, Политики, Процедури и инструкции касаещи избора, инсталацията, администрацията, защитата, експлоатацията и поддръжката на информационните системи, класификацията на информацията, управлението на риска, управлението на инциденти, непрекъснатостта на дейността и други.

(2) Правата и задълженията на служителите в ОДЗ по отношение мрежовата и информационна сигурност, се определят в разработените документи.

Чл. 11. (1) Приетите Правила за класификация на информацията в ОДЗ изискват да се определи нивото на класифициране на всяка информация (електронна или на хартиен носител), както и на всички ресурси участващи в създаването, трансфера и съхранението на информацията.

(2) Всяка информация и ресурс трябва да е с поставен етикет на класификация.

(3) При обмен на информация се използва класификация TLP (traffic ight protocol) съгласно Правилата.

Чл. 12. (1) Всички информационни активи в ОДЗ се идентифицират в опис със следните групи: сървъри, компютри, периферия, комуникационни устройства, информационни системи, документи, услуги и други.

(2) За всеки актив се описва информация, която има отношение към информационната сигурност.

(3) Описът с информационните активи се поддържа динамично при настъпване на обстоятелство за нов или бракуван актив, като се преглежда минимум веднъж годишно за актуалност.

Чл. 13. (1) С цел предприемане на адекватни мерки по управлението на информационната сигурност, в ОДЗ е приет процес по управление на рисковете.

(2) Процесът включва идентификация на заплахите, определяне на наличните мерки за защита, оценяване на риска, приоритизиране на риска.

(3) Определен е прагът на приемливия риск в ОДЗ, като всички рискове над него се включват в план за намаляване на риска, който изисква нови мерки за защита, с определени отговорници, срокове и оценка на остатъчния риск;

(4) Извършва се документиране и докладване на процесите при управление на рисковете, свързани с мрежовата и информационна сигурност, съгласно Стратегия за управление на риска в ОДЗ;

(5) За гарантиране високото ниво на управление на сигурността в ОДЗ, анализът и оценката на риска се извършва регулярно, но не по-малко от веднъж годишно.

Чл. 14. За управлението на взаимоотношенията с доставчиците на стоки и услуги в Дирекцията са приети правила с които се изисква да се определят набор от мерки касаещи сигурността на веригата от доставки, достъпа до информационни ресурси, дефиниране на параметри на услугите и доставките, контрола, както при неизпълнение на договорите и други.

Чл. 15. (1) Управлението на логическия достъп до информационните ресурси на ОДЗ е описано в приетите „Вътрешни правила за потребителите на компютърната и информационната среда“.

(2) Достъп до информационни ресурси на служителите се предоставя съобразно служебните задължения и необходимостта.

(3) На всеки служител му се предоставя персонален акаунт с парола съответстваща на Вътрешните правила и Наредбата за минимални изисквания за мрежова и информационна сигурност;

(4) При необходимост от достъп до информационни активи извън мрежата на ОДЗ се използват само канали с висока степен на защита като Virtual Private Network (VPN) u най-малко двуфакторна автентикация.

Чл. 16. За оценка ефективността на мерките за сигурност и на услугите се извършва мониторинг с който се анализират данните с предприемане на превантивни мерки.

Чл. 17. Управлението на негативните събития и инцидентите се извършва на база приетите Правила, с които се определят редът за реакция, докладване на съответните нива, прекратяване на действието на инцидента и последващи действия по събиране на доказателства и анализ.

Чл. 18. Всички системни записи от информационните системи се съхраняват минимум година в среда с ограничен достъп.

Чл. 19. Целостта и наличността на информацията се гарантира с Правилата за резервиране и архивиране, които изискват да се съхраняват копия на всички информационни системи в ОДЗ с определени параметри. Копията се тестват веднъж годишно.

Чл. 20. В ОДЗ, на основание чл.8, ал.1 от Наредба № 8121-з-647/ 01.10.2014 г. за правилата и нормите за пожарна безопасност при експлоатация на обектите, са разработени Досиета за ОДЗ и териториалните звена – Общинските служби по земеделие, които осигуряват минимизиране на негативните въздействия по отношение на мрежовата и информационната сигурност при възникване на екстремни ситуации.

Чл. 21. Контролът и оценката на нивото на мрежовата и информационна сигурност се извършва чрез организиране и провеждане на вътрешни одити в ОДЗ веднъж годишно.

Чл. 22. Ръководителите и служителите в ОДЗ са длъжни да познават и спазват разпоредбите на тази Политика.

Чл. 23. Политиката се разглежда и оценява веднъж годишно с оглед адекватноста и ефективноста й.

Заключителна разпоредба

Параграф единствен. Тази Политика е разработена съгласно Наредба за минималните изисквания за мрежова и информационна сигурност.