РЕПУБЛИКА БЪЛГАРИЯ
Министерство на земеделието, храните и горите
Областна дирекция „Земеделие”-Варна

УТВЪРЖДАВАМ:

ИНЖ. ЙОРДАН ЙОРДАНОВ
Директор ОД ”Земеделие”-ВАРНА
Съгласно Заповед № РД 19-04-50/13.08.2019 г.

ПОЛИТИКА ПО ИНФОРМАЦИОННА СИГУРНОСТ

В България близо 60% от домакинствата и над 90 % от предприятията имат достъп до Интернет, като 50% от предприятията използват автоматизиран обмен на данни с външни ИКТ системи. Почти цялата комуникация на публичната администрация с бизнеса е само електронна, нарастват и услугите към гражданите които се извършват предимно по интернет. Интернет свързаността и скоростта на информационните канали непрекъснато расте – България е в групата на топ 20 в света по скоростен интернет, и между първите по степен на въвеждане на високо скоростен, което предоставя нови възможности за отдалечени и облачни услуги, но и нови възможности за мащабно и злонамерено използване.

Кибер атаките *са директна заплаха за сигурността на гражданите и функциониране на държавата, икономиката, обществото, науката и образованието. Те могат да бъдат извършени от разстояние, с прости и ефективни механизми и минимални ресурси, да причинят значителни поражения с нанасяне на материални и дори човешки загуби. Кибер атаките нямат национални, културни или юридически граници.*

Рисковете и заплахите *в кибер пространството са трудни за дефиниране поради сложността за определяне на източника на въздействие, целите и мотивите, бързото ескалиране на заплахата и трудно предвидимите перспективи за развитие, сложността и интензивността на съвременните комуникационни и информационни процеси, динамиката на логическите и физическите връзки и неопределеността на процесите.*

Раздел I: ОБЩИ ПОЛОЖЕНИЯ

1. Ръководството, в лицето на директора на Областна дирекция „Земеделие“-Варна /Дирекцията/, официално декларира Политиката по информационна сигурност на информационната система на Дирекцията.
2. Политиката е документирана и огласена пред служителите, които имат достъп до информацията и информационните системи на Дирекцията. Политиката се прилага в рамките на институцията.
3. Служител по информационна сигурност ръководи и контролира дейностите, свързани с постигане на мрежова и информационна сигурност на Дирекцията в съответствие с нормативната уредба, политиките и целите за мрежова и информационна сигурност. Служителят се определя със заповед на директора на Дирекцията, а неговите функции се определят с длъжностна характеристика, вътрешни правила и заповеди на директора на Дирекцията.

4. Настоящата политика задава рамката на система от мерки, насочени към:
   - гарантиране на конфиденциалност на информацията, чрез прилагане на одобрени ограничения върху достъпа и разкриването на информация;
   - осигуряване на цялостност на информацията, чрез защита срещу неправомерни изменения или разрушаване на информация;
   - осигуряване на достъпност на информацията, чрез осигуряване на надежден и навременен достъп;
   - постигане на отчетност на информацията, чрез въвеждане на контрол върху достъпа и правата върху информационните ресурси.

Раздел II: ЦЕЛИ

5. Целите на настоящата политика са:
   - осигуряване на непрекъснатост на работните процеси;
   - минимизиране на рисковете за сигурността на информацията, причиняващи загуби или вреди на Дирекцията;
   - минимизиране на степента на загуби или вреди, причинени от пробиви в информационната сигурност;
   - осигуряване на необходимите ресурси за поддържане на ефективно управление на информационната сигурност;
   - информиране на служителите за техните отговорности и задължения по отношение на информационната сигурност;
   - осигуряване на съответствие с нормативни изисквания.

6. Ръководството на Дирекцията ще прилага следните основни принципи при управление на информационната сигурност:

6. 1. От законова гледна точка:
   - защита на данни и неприкосновеност на лична информация;
   - опазване на архивите на институцията;
   - защита на авторски права, търговска информация и други права върху интелектуална собственост.

6.2. От общоприетите добри практики за информационна сигурност:
   - разработване на политика по информационна сигурност;
   - разпределяне на отговорностите по информационна сигурност;
   - обучение по информационна сигурност;
   - докладване на инциденти, свързани със сигурността;
   - управление непрекъснатостта на работа;

7. Стратегическа цел на Дирекцията за въвеждане на тази политика е, че тя дефинира мястото и по отношение на мисията и целите на Дирекцията и установява общи правила за поведение.

Раздел III: ОБХВАТ НА СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

8. Системата за управление на информационната сигурност обхваща:
   - всички документи - електронни и на хартиен носител;
   - бази данни;

- компютри – настолни и преносими;
- софтуерни активи;
- локална мрежа и мрежи в изнесените работни места;
- всички WEB базирани и други информационни системи на Дирекцията;
- носители на информация (дискови масиви,дискове, USB памети и др.);
- устройства за копиране и предаване на данни;
- комуникационни устройства;
- инфраструктура на Дирекцията (електрозахранване, кабели за локална мрежа и др.);
- служители.

9. Системата за управление на информационната сигурност обхваща всички структурни звена и изнесени работни места на Дирекцията.

10. Тази политика не се отнася за документи и процеси свързани с класифицирана информация и попадащи под обхвата на Закона за защита на класифицираната информация.

Раздел IV: ПРИОРИТЕТИ

11. Ръководството на Дирекцията насочва внимание и полага усилия:

- критичната (чувствителната) информация и системи да бъдат подлагани на редовен анализ по отношение на риска;
- за критичните (чувствителни) информационни ресурси и системи да бъдат определени служители, отговорни за конкретните работни приложения, компютри и мрежи;
- информацията да бъде класифицирана по начин, който показва нейната критичност и чувствителност;
- служителите да бъдат информирани и да осъзнават проблемите на информационната сигурност;
- да бъде създадена организация на работа, която гарантира спазване на авторски права на компютърния софтуер, както и условията за работа с тях.
- нарушаването на политиката по сигурността и евентуалните недостатъци в системата за информационна сигурност да бъдат докладвани;
- информационните ресурси да бъдат защитавани от гледна точка на изискванията за конфиденциалност, цялостност и достъпност.

12. Въвеждането и спазването на политиката по информационна сигурност цели да се забранят:

- използването на информацията и системите на организацията без оторизация или за цели, които не са свързани с дейността й;
- изнасяне на оборудване или информация от изнесените работни места без оторизация;
- неоторизирано копиране на информация и софтуер;
- компрометиране на пароли (например със записване или разпространяване);
- използване на персонална информация за други цели, освен ако няма изрична оторизация;
- фалшифициране на доказателства в случай на инцидент.

- отправяне на неприлични, дискриминационни или нападателни изявления, които могат да бъдат противозаконни (например с използване на електронна поща или интернет);
- разпространение на незаконни материали (например с неприлично или дискриминационно съдържание).

Раздел V: ОТГОВОРНОСТИ

13. За осъществяване на настоящата политика и за осигуряване на информационната сигурност, ръководството на Дирекцията определя следните отговорности:

13.1. Служителят по т. 3:

- формулира, преглежда и предлага за изменение Политиката по информационна сигурност;
- оценява потребностите и планира необходимите ресурси за осигуряване на информационната сигурност;
- разпределя ролите и отговорностите, свързани със сигурността на информацията, изготвя план за действие и планове за обучение;
- координира прилагането на мерки за защита и информационна сигурност.
- отговаря за управление и поддържане на интранет, електронна поща, сървъри, локална мрежа, архивиране, техническа защита (софтуер и хардуер) от вреден софтуер; нива на достъп; проследимост на включване и опити за включване; изготвяне и поддръжка на цялостната документация, свързана с администрирането на информационната система и нейните подсистеми.
- изпълнява възложени дейности, свързани с прилагане на Политиката и мерките по осигуряване на информационна сигурност;
- прилага набелязаните мерки за поддържане на информационната сигурност и следи за тяхната ефикасност при изменения в информационната система.
- при възникнала необходимост предлага нови, спешни и ефикасни мерки за подобряване на сигурността.

13.2. Потребители:

- потребителите на информационната система, се задължават да следват процедурите, инструкциите и заповедите, свързани с информационната сигурност, да докладват за проблеми и инциденти в информационната система на системния администратор.

Раздел VI: ОЦЕНКА НА РИСКА

14. Оценката на риска се прилага за всеки актив на Дирекцията или извън нея, обхванат от споразумение с трета страна. Оценката на риска се прилага към цялата информационна система и включва приложения, мрежа, всеки процес или процедура, чрез които системата се администрира и/или поддържа.

15. Идентифицирането и оценката на риска се извършва на базата на разработена и утвърдена Стратегия за управление на риска в МЗХГ.

16. Постоянна работна група, определена със заповед № РД 18-10-130/30.03.2018 г. на директора на Дирекцията, извършва идентифициране, оценка и управление на

рисковете, свързани с информационната сигурност на Дирекцията, като документира процеса в утвърдената форма – риск-регистър.

17. Резултатите от оценката на риска определят мерките за контрол за намаляване на риска в съответствие с нивата на риска.

18. Оценката на риска се извършва периодично, за да бъдат отчетени измененията в изискванията за сигурност, активите, заплахите, уязвимостите, въздействията или други настъпили промени.

Раздел VII: ВЪТРЕШНА ОРГАНИЗАЦИЯ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

19. Ръководството на Дирекцията провежда политика за координиране на цялата дейност в организацията по внедряването и поддържането на мерките за защита.

20. Разпределяне на отговорностите по сигурността на информацията се извършва в съответствие с приета Политиката по информационна сигурност.

21. Отговорностите на служителите се определят в съответствие с настоящата политика, във вътрешни правила, заповеди или в длъжностните им характеристики.

22. Служителят по т. 3 предлага на Директора за одобрение разпределението и документирането на отговорностите за изпълнението на следните дейности:

- защита на активите;
- поддръжка на ключови ресурси на организацията - мрежа, сървъри, потребителски заявки;
- закупуване, изменения и поддръжка на софтуерните ресурси;
- закупуване, изменения и поддръжка на хардуерни компоненти;
- правила за поддръжка на инфраструктурата, вътрешния ред и контактите с външни организации;
- управление на инциденти;
- непрекъснатост на дейността;
- сключване на споразумения за поверителност с трети страни и изисквания за защита на поверителната информация на организацията.

Раздел VIII: УПРАВЛЕНИЕ НА АКТИВИТЕ

23. Политиката се отнася до служители, договарящи страни, консултанти, временно работещи за Дирекцията (стажанти) и други, включително и служители на трети страни. Тази политика се отнася до цялото информационно оборудване, собственост или използвано от Дирекцията.

24. Политиката на Дирекцията за използване на активите цели не да налага ограничения, противоречащи на установената култура на откритост и доверие, а да защитава служителите на Дирекцията, нейните партньори и самата нея от незаконни и увреждащи действия, извършени предумишлено или несъзнателно.

25. Системите, свързани с интернет, локална мрежа, включително компютърното оборудване, приложния софтуер, операционните системи, средствата за съхранение на информация, електронната поща и други са собственост на Дирекцията. Тези системи са предназначени да се използват за целите на дейността и в интерес на организацията.

26. Данните, които потребителите обработват и съхраняват при изпълнение на

служебните се задължения са собственост на Дирекцията и МЗХГ.

27. За всяка друга информация, съхранявана на технически средства на Дирекцията не се гарантира конфиденциалност. Служителите са задължени да правят добра преценка относно разумността на съхраняване на информация върху служебни технически средства за лична употреба.

28. За целите на сигурността и поддръжката на мрежата, системният администратор наблюдава оборудването, системите и мрежовия трафик по всяко време.

29. Дирекцията си запазва правото чрез системния администратор да деинсталира всякакъв софтуер или файлове, които не са свързани със служебните задължения на потребителя. Примери за такъв софтуер или файлове включват, но не се ограничават до: игри, музикални файлове, файлове с изображения, споделени и безплатни програми, и др.

30. Дирекцията си запазва правото периодично да одитира мрежите и системите, за да провери спазването на тази политика.

31. Потребителите, имащи достъп до информацията, разположена в системите свързани с интернет/локална мрежа са длъжни да спазват политика за чисто бюро, чист екран и защита на ненадзиравани устройства.

32. Служителите трябва да прилагат изключително внимание когато работят с електронната поща, за да се предпазят от вируси, троянски коне и друг вредоносен софтуер.

Раздел IX: СИГУРНОСТ, СВЪРЗАНА С ЧОВЕШКИТЕ РЕСУРСИ

33. Сигурността на човешките ресурси на Дирекцията е насочена основно към осъзнаване на необходимостта от осигуряване на информационната сигурност чрез адекватно дефиниране на отговорности и обучение.

34. Администрирането на човешките ресурси обхваща целия процес - от проучване на кандидатите, назначаване, определяне на задълженията, промяна на длъжността и до прекратяване на договорите включително и се извършва в съответствие с Вътрешните правила за подбор, назначаване, обучение, оценка на трудовото изпълнение и професионалното развитие на служителите на Дирекцията.

35. Всички служители на Дирекцията се задължават да спазват утвърдените правила и процедури, свързани с информационната сигурност, определени в политиката и вътрешните актове на Дирекцията. Това обстоятелство се удостоверява чрез декларация, която служителите подписват при постъпване на работа, съгласно заповед на директора на Областна дирекция „Земеделие“-Варна.

36. В договорите с лица, по силата на които последните обработват информация на Дирекцията, задължително се включват клаузи за спазване на конфиденциалност.

Раздел X: ФИЗИЧЕСКА СИГУРНОСТ, СИГУРНОСТ НА ЗАОБИКАЛЯЩАТА СРЕДА И КОНТРОЛ НА ДОСТЪПА

37. Информационните системи, които поддържат критични за Дирекцията дейности, притежават подходяща физическа сигурност. Никакви конфиденциални материали в електронен формат не се оставят в неконтролирана среда и са защитени срещу случаен

достъп.

38. Оборудването, което поддържа критични функции, се защитава физически от заплахи за сигурността и влияние на рискове от околната среда за предотвратяване на загуби, щети или излагане на риск на активи и прекратяване на основни дейности. Помещенията, в които е разположено такова оборудване са със строго ограничен и контролиран достъпът.

39. Защитата на физическата сигурност се базира на непрекъснатостта на външната граница (конструкция от плоча до плоча) и на подходящ контрол на достъпа (ключове за ограничен достъп, входни точки за служителите, секретни ключалки, дневник за достъп, видеонаблюдение).

40. Изнасянето извън сградите на Дирекцията на информационните активи /собственост на Дирекцията/ изисква разрешение от директора и подлежи на проверка.

41. Служебна информация не се оставя без надзор или контрол, което означава видима на екран.

42. Когато използването на дадено оборудване се прекрати, всички ключове, идентификационни карти и други устройства и пароли за достъп се връщат и отчитат.

43. Физическият достъп до ИТ съоръженията и комуникационното оборудване на Дирекцията се извършва от и/или в присъствие на служители на Дирекцията.

44. Средствата за контрол на физическата сигурност се използват и при защита на копирни машини, факсове и мрежови принтери.

45. Всички информационни системи на Дирекцията работят във физически условия, дефинирани от техните производители.

46. Дирекцията създава поддържа и осигурява условия за безопасна работа в съответствие със Закона за здравословни и безопасни условия на труда.

Раздел XI: РАЗРАБОТВАНЕ, ВНЕДРЯВАНЕ И ПОДДЪРЖАНЕ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

47. Политиката на Дирекцията по разработване, внедряване, изменение и поддържане на информационните системи е базирана на принципа на превантивната оценка на риска от измененията, включително ъпгрейд на съществуващи и внедряване на нови елементи от системата, разделение на средата за изпитване от действащата информационна система и планирана поддръжка на цялата информационна система.

48. С цел предотвратяване на грешки, загуба, неразрешено изменение или използване на информация в приложни информационни системи, се прилагат механизми за контрол върху входните данни, вътрешната обработка и изходните данни.

49. Разработването и внедряването на информационни системи се предхожда от анализ за необходимостта от тях, както и от ясно и конкретно дефиниране на процесите, които съответните системи предстои да обслужват.

Раздел XII: УПРАВЛЕНИЕ НА ИНЦИДЕНТИ И ПОДОБРЯВАНЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

50. В Дирекцията следва да се събират данни и да се извършва анализ на вида и броя на инцидентите, на направените разходи по разрешаване на инцидентите. Целта е да се идентифицират повтарящите се инциденти или инцидентите с голямо влияние, да се ограничат честотата, щетите и загубите от появата им в бъдеще.

Раздел XIII: ОСИГУРЯВАНЕ НА НЕПРЕКЪСНАТОСТТА НА ДЕЙНОСТТА

51. Ръководството на Дирекцията оценява необходимостта от планиране непрекъснатостта на дейността. Осъзнава, че има значителен риск за неговите критични процеси при потенциални и неочаквани разрушителни събития. Увеличаващото се развитие на процеси, базирани на технологии и силната зависимост от информационните технологии, е основание за създаване на план за непрекъснатост на работа.

52. Дирекцията създава условия и следи за непрекъснатост на работата на критичните ресурси на системата при настъпване на сериозни неблагоприятни условия и опасност за прекъсване, по-голямо от 8 часа.

Раздел XIV: ПРИДОБИВАНЕ И ПОЛЗВАНЕ НА ЛИЦЕНЗИ

53. Дирекцията създава организация на работа, която гарантира спазване на авторски права на компютърния софтуер, както и условията за работа с тях. Институцията предприема всички необходими действия за предотвратяване на копирането на лицензиран софтуер от потребителите, както и използването на свързана с него документация в изнесените работни места или на друго място, освен ако не съществува изрично разрешение за това, съгласно договора с лицензодателя.

54. Служителите използват софтуера по начин, който съответства на условията в договора, с който са предоставени лицензите.

55. Компютрите на Дирекцията са активи, нейна собственост, използват лицензиран софтуер и са защитени от вируси.

56. Забранява се на потребителите да внасят софтуер отвън и да го инсталират на своите компютри. Ползваният от Дирекцията софтуер не може да бъде изнасян от потребителите и качван на други компютри.

57. Всички потребители използват наличния софтуер, при спазване на условията на съответните лицензионни договори.

Раздел XV: ЗАЩИТА НА АВТОРСКИТЕ ПРАВА

58. Политиката на Дирекцията за защита на авторските права е изцяло съобразена със Закона за авторското право и сродните му права.

Раздел XVI: ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

59. Политиката на Дирекцията за защита на личните данни е изцяло съобразена със Закона за защита на личните данни.

Раздел XVII: ЗАКЛЮЧЕНИЕ

60. Настоящата политика се предоставя на трети страни, които имат достъп до информацията и системите на организацията, с цел запознаване и недопускане на инциденти, които да поставят в риск сигурността.

61. Настоящата политика се преразглежда от Съвета, с цел гарантиране на нейната уместност, адекватност и ефективност регулярно, но не по-малко от веднъж годишно и в случай на законови, организационни и технически промени.

62. Всеки служител, който прецени, че има злоупотреба с настоящата политика, уведомява незабавно служителя па т.3.

63. Ролите във връзка с отговорностите по провеждане на политиката по информационна сигурност се разпределят за изпълнение от конкретни длъжностни лица чрез правила, заповеди, допълнение на длъжностни характеристики или по друг подходящ начин.

64. Служителите на Дирекцията се задължават да спазват всички вътрешни актове, издадени във връзка с информационната сигурност.

65. служителят по т. 3 изготвя, а директорът на Дирекцията одобрява план за действие за постигане на заложените в политиката цели чрез определяне срокове, отговорни структурни звена и/или длъжностни лица.

Настоящата политика е утвърдена със заповед № ……..……..г. на директора на Дирекцията, и влиза в сила от …….. …….2019 г.

Приложение № 1
към чл. 35

ДЕКЛАРАЦИЯ ЗА КОНФИДЕНЦИАЛНОСТ

От: ……, в качеството на служител на Областна дирекция “Земеделие“-Варна/упълномощен представител на **……,** със седалище и адрес на управление: град ……, ул. ”…” № …, ЕИК …, представлявано от ….., ИЗПЪЛНИТЕЛ по договор за **…** със ОБЛАСТНА ДИРЕКЦИЯ „ЗЕМЕДЕЛИЕ“-ВАРНА**,** гр. Варна, ул. ”Д-р Пискюлиев” № 1, БУЛСТАТ 175811402, представлявана от инж. Йордан Йорданов – Директор на Областна дирекция “Земеделие“- Варна, като ВЪЗЛОЖИТЕЛ

на основание чл. ... от Договора, декларирам, че :

1. Се задължавам да не разгласявам конфиденицална информация, получена от ВЪЗЛОЖИТЕЛЯ, станала ми известна в процеса на работата ми по изпълнението на Договора.

2. Конфиденциална информация по смисъла на настоящата Декларация е всяка информация, получена в писмен, устен или електронен вид, която се обработва в Дирекцията, включително информация относно лични данни, собственост, сделки, финансовото състояние и други за всички лица, за които се отнася тази информация.

3. Разгласяване на конфиденциална информация по смисъла на настоящата Декларация представлява всякакъв вид устно или писмено изявление, предаване на информация на хартиен, електронен или друг носител, включително по поща, факс или електронна поща, както и всякакъв друг начин на разгласяване на информация, в това число чрез средствата за масово осведомяване, печатните издания или Интернет.

4. Задължението за запазване на конфиденциалност има действие от датата на действие на договора и е без ограничение във времето.

5. Задължавам се да пазя конфиденциалната информация добросъвестно, за да предпазя разпространяването и публикуването й от лица, които нямат правото да я разпространяват и публикуват.

6. Задължението за запазване на конфиденциалност няма да се прилага по отношение на информация, която е предадена по искане на компетентен орган, както и по отношение на информация, която е била публично оповестена или е била придобита от трети лица.

7. Задължавам се да върна на ВЪЗЛОЖИТЕЛЯ всички предоставени ми от него хартиени и/или електронни документи, предоставени ми по повод изпълнение на задължения по Договора.

Декларатор: .....
(трите имена, длъжност, подпис)