УТВЪРДИЛ: /П/
ИНЖ. ГЕОРГИ ГУГУЧКОВ
ОБЛАСТЕН УПРАВИТЕЛ НА
ОБЛАСТ ВЕЛИКО ТЪРНОВО
СЪГЛАСНО ЗАПОВЕД № РД-01-05-67/10.07.2023 г.

В Ъ Т Р Е Ш Н И П Р А В И Л А

за правата и задълженията на служителите по мрежова и информационна сигурност в Областна администрация Велико Търново

I. ОБЩИ ПОЛОЖЕНИЯ

1. Настоящите вътрешни правила са разработени на основание чл. 5, ал. 1, т. 7 от *Наредбата за минималните изисквания за мрежова и информационна сигурност* (Наредбата) и са в съответствие с изискванията както на Наредбата, така и на внедрената *Интегрирана система за управление* (ИСУ) по отношение на сигурността на информацията и международен стандарт ISO/IEC 27001:2013.

1.1 Настоящите вътрешни правила се приемат с цел намаляване на риска от инциденти, умишлено или неумишлено предизвикани от служители на администрацията като указват техните права и задължения за осигуряване физическата защита на предоставените информационни активи; за използване на компютърната техника, периферните и преносими устройства, на сменяемите носители; за достъп до ресурсите на локалната мрежа; за генериране и съхранение на паролите; за достъп до интернет; за работа с електронна поща; за работа със софтуера, вкл. със системата за документооборот, другите вътрешноведомствени и централизираните системи.

2. Областният управител носи пряка отговорност за мрежовата и информационната сигурност (МИС). Ръководството създава условия за прилагане на комплексна система от мерки за управление на МИС, включително физическата сигурност на информационните и комуникационните системи; осигурява необходимите ресурси за прилагане на организационни, технически и технологични мерки, гарантиращи високо ниво на мрежова и информационна сигурност; координира и преглежда внедрената ИСУ; определя, документира и разпределя отговорности по изпълнението, контрола и информираността за всички процеси и дейности, свързани с развитието, поддръжката и експлоатацията на информационните и комуникационните системи, като се спазва принципът, че едно лице не може да контролира собствената си дейност.

3. Администрацията работи с информация, която е класифицирана в съответствие с изискванията на нормативните актове, нейната стойност, критичност и чувствителност към неоторизирано разкриване или модифициране, регламентирана в *04 ОД-08.02 Списък на данните, фактите и предметите, които се категоризират като държавна тайна, служебна тайна и чувствителна информация на Областна администрация Велико Търново*

4. Всички вътрешни правила и инструкции, свързани със сигурността на информацията, са описани в *04 ОД-18.01 Регистър на основното приложимо за Областна администрация Велико Търново законодателство по отношение на сигурността*.

5. В случай на проблеми при работа с информационните системи, хардуера и комуникациите, следва чрез отговорните служители да се търсят контакти с доставчиците от *04 ОД-15.01 Регистър на утвърдени доставчици за техническа поддръжка на системи и средства за обработка на информация в Областна администрация Велико Търново*.

II. СИГУРНОСТ ПО ОТНОШЕНИЕ НА ПЕРСОНАЛА И АКТИВИТЕ

6. Назначаването на работа в администрацията се осъществява в съответствие с приложимите закони и подзаконови нормативни актове, професионалната етика и съобразно изискванията, свързани с дейността на служителя - класификацията на информацията, до която има достъп, и предполагаемите рискове.

7. Ръководството на администрацията определя и разпределя отговорностите и задълженията по мрежова и информационна сигурност в съответствие с утвърдените политики чрез организационни процедури *04 ОП-07 Организиране на сигурността на информацията, 04 ОП-07 Сигурност на човешките ресурси*, заповеди, процедури, инструкции, длъжностни характеристики и договорни отношения.

8. Всички служители на администрацията подписват *04 ОД-07.01 Декларация за поверителност и лоялност*, в която се регламентират техните отговорности по отношение на сигурността на информацията в съответствие с класификацията на чувствителната информация и *04 ОД-08.02 Списъка на данните, фактите и предметите, които се категоризират като държавна тайна, служебна тайна и чувствителна информация, които не подлежат на публично огласяване*.

9. Новопостъпилите служители в рамките на началния инструктаж се запознават с правата и задълженията си по отношение на мрежовата и информационна сигурност, залегнали в настоящите вътрешни правила, за което подписват служебна бележка.

10. Служителите носят дисциплинарна отговорност при пробив/срив в сигурността на информацията. Прилагането на дисциплинарния процес в администрацията е част от превенцията за предотвратяване нарушения на политиките и процедурите по мрежова и информационна сигурност.

11. По утвърдена годишна *Програма за обучение на персонала*, вкл. по аспектите на сигурността, за всички служители трябва да се провежда периодичен инструктаж за повишаване вниманието на служителите по отношение на мрежовата и информационна сигурност; за отговорните служители за мрежовата и информационна сигурност трябва да се осигури професионално обучение за повишаване квалификацията в съответствие с използваната техника и технологии; при внедряване на нов вид дейност и/или услуга трябва да се провежда специализирано обучение.

12. За всички информационни активи, материални и нематериални, дълготрайни и краткотрайни, които са с полезна стойност за администрацията, се назначават собственици, на които се възлагат отговорности за защитата им, за правилното съхранение и допустимото им използване през целия жизнен цикъл.

13. Определя се еднозначно кой служител за кои информационни активи отговаря. За всеки актив към момента на придобиването му се определя материално отговорно лице (МОЛ), уточнява се местонамирането му и се завежда в счетоводната информационна система. За приемането на компютърна техника и периферни устройства, както и при промяна на някое от тях, служителите подписват **Приложение 1** *Протокол за предаване на информационни активи*.

14. Всеки служител отговаря за целостта на компютърната и периферна техника, за програмните продукти и данни, необходими за работата му, инсталирани на компютъра на неговото работно място или ползвани от него на сървъри от локалната мрежа, съобразно дадените му права.

15. Забранява се на външни лица да работят с компютърната и мрежова техника на администрацията. Допускат се изключения за представители на доставчици при първоначална инсталация на компютърна, мрежова, комуникационни, периферна техника и софтуер и при сервизна намеса на място, но задължително в присъствие на СМИС.

16. Контрол за местоположението, притежанието и целостта на активите се извършва в рамките на годишната инвентаризация.

17. При прекратяване на служебните/трудовите правоотношения връщането на активите се удостоверява с *04 ОД-08.03 Протокол за напускане/уволнение на персонал*, който се подписва от уволнения/напускащия служител и отговорни представители на администрацията. Служителят подписва още, че е инструктиран да спазва изискванията за поверителност.

III. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ ЗА ОСИГУРЯВАНЕ НА ФИЗИЧЕСКА ЗАЩИТА НА ИНФОРМАЦИОННИТЕ АКТИВИ

Пропускателен режим

18. С цел осигуряване физическа защита на сградата, безопасност и охрана на имущество, администрацията използва система за видеонаблюдение и система за контрол на достъпа (пропускна система).

19. На всеки служител се предоставя магнитна карта, с която се осигурява както влизането в сградата, така и движението вътре в администрацията.

20. Магнитната карта трябва да се поднася пред четеца от пропускната система безконтактно, без огъване, да се експлоатира и съхранява по начин, гарантиращ целостта и, да се пази от нагряване, намокряне, прегъване, пречупване и друго, което би могло да я повреди. Не се допуска персоналната магнитна карта да се преотстъпва за ползване от други лица.

21. Магнитната карта трябва да се върне на отговорния счетоводител при прекратяване на служебно или трудово правоотношение. В случай на повреда, загуба или кражба, своевременно трябва да се уведомят ССИ и/или отговорния счетоводител. При повреда, за която служителят има вина, и при загубване, се заплаща стойността на картата.

22. Не се допуска нерегламентирано изнасяне на имущество от администрацията.

23. При смущаващо поведение на външни посетители трябва да се реагира своевременно като се информира дежурен служител "Гише пропуски".

Лична идентификационна карта

24. При упражняване на дейността, всеки служител трябва да носи като видима идентификация лична идентификационна карта (бадж).

Защита на работните помещения

25. Работните помещения се защитават пропорционално на класификацията на съхраняваната чувствителната информация и на средствата за обработката й, посредством заключване на помещенията, на металните шкафове, на касите, на решетките на вратите, както и посредством използване на решетки и затъмнители за прозорци.

26. В определените им помещения, на служителите са осигурени оборудвани работни места при спазени изискванията за здравословни и безопасни условия на труд.

27. Служителите не трябва да оставят без надзор техническите средства, служебните документи, лични вещи, пари и други.

28. Всички помещения в сградата на администрацията в извънработно време и през почивните и празнични дни трябва да бъдат заключени, а прозорците - затворени и затъмнени.

29. Всички служители преди напускане на работните помещения трябва да изключват компютърната техника, да изключат от контакта отоплителните или други електрически уреди, с които са работили.

Осигуряване на пожарна безопасност

30. Служителите трябва да спазват стриктно противопожарните изисквания, да познават употребата на различните видове пожарогасители, къде се намират и как се действа с тях.

31. Служителите трябва да реагират при опасност от пожар в съответствие с препоръките, дадени в рамките на периодичните инструктажи по безопасност и здраве при работа, вкл. при задействане на алармата от пожаро-известителната система.

32. Забранено е ползването на открит огън в помещенията, внасянето на взривни и запалителни материали в сградата без необходимите документи.

33. Забранено е тютюнопушенето в помещенията на администрацията. Разрешените зони за пушене са извън административната сграда.

IV. СИГУРНОСТ ПРИ РАБОТА С УСТРОЙСТВА

34. Устройствата трябва да бъдат разположени и защитени така, че да се предотвратят загуби, повреди, кражби или компрометирането им, които биха довели до евентуално прекъсване дейности на администрацията.

35. Средствата за обработване на информация, особено тези, които се занимават с чувствителни данни, трябва да бъдат разположени внимателно, за да се минимизира излишният достъп до работните зони и да се намали рискът информацията да бъде видяна от неоторизирани лица по време на нейното използване.

36. Не се допуска неоторизирано копиране на документи и информация, записване на звук с цифрови камери, смартфони и други възпроизвеждащи устройства.

37. Не е допустимо хранене, пиене и пушене в непосредствена близост до средствата за обработване на информация.

38. Обслужване и ремонт на устройствата трябва да се извършва само от оторизиран персонал и от представители на фирмите, отговорни за поддръжката им.

39. Където е необходимо, температура и влажност трябва да бъдат наблюдавани за условия, които могат да повлияят неблагоприятно на работата на средствата за обработване на информация.

Изнасяне на собственост

40. Устройства, информация или софтуер не се изнасят от администрацията без разрешение на ръководството.

41. При изнасяне на презаписваеми носители, предишното им съдържание, ако не е нужно повече, трябва да се изтрива.

42. Активи /канцеларско оборудване, компютърни устройства, преносими компютри, принтери, носители и др./ се изнасят от администрацията след като се опишат по вид и количество в *Служебна бележка за изнасяне на активи* и се получи разрешение и подпис от главния секретар или от служителя по сигурността на информацията (ССИ). Дежурен служител "Гише пропуски" проверява изнасяните активи, съхранява служебната бележка и удостоверява връщането им.

43. Възможни са внезапни проверки за откриване на неразрешено изнасяне на имущество.

Сигурност при работа с мобилни устройства

44. Когато мобилните устройства за съхраняване и обработване на служебна информация (преносими компютри, таблети, мобилни телефони и др.) се използват извън помещенията на администрацията - на обществени места, в заседателни зали и други незащитени зони, те трябва да имат защита (например използване на криптографски техники и на тайна информация за автентификация), за да се избегне неоторизиран достъп или разкриване на информация, съхранявана и обработвана от тези устройства. Подробна информация виж в **Приложение 2** *Инструктаж за обезпечаване сигурността на оборудването извън инфраструктурата на Областна администрация Велико Търново*.

45. Преносимите устройства, принадлежащи на администрацията се използват само за работа, извършвана от и в интерес на администрацията.

46. Мобилните устройства трябва да бъдат и физически защитени от кражба, особено когато са оставени в автомобили или други превозни средства, в хотелски стаи, конферентни и заседателни зали.

47. Преносимите компютри се носят като ръчен багаж и при пътуване се прикриват, където е възможно.

48. Устройствата, които съдържат важна, чувствителна или критична информация за дейността, не трябва да бъдат оставяни без надзор и, когато е възможно, трябва да бъдат физически заключвани, да се използват специални заключващи механизми.

49. Всички файлове, изтеглени от служителите (включително от интернет и електронна поща) се проверяват за злонамерен софтуер.

50. До служебните мобилни устройства не трябва да се допускат неоторизирани лица, включително приятели и членове на семейството.

51. Забранено е съобщаването на чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Сигурно унищожаване на устройства и носители

52. Излезлите от употреба или повредени устройства и носители, съдържащи чувствителна информация, се унищожават по сигурен начин и безопасно чрез механично счупване, изгаряне, нарязване или информацията се изтрива надеждно с използване на техники, които правят оригиналната информация невъзстановима.

53. Действията се извършват в присъствието на поне двама служители и се документират в *04 ОД-08.03 Протокол за унищожаване на информационни носители*.

54. Ненужните документи и черновите на хартиен носител се унищожават посредством шредер, като обобщена информация за процеса се документира периодично в *04 ОД-08.03 Протокол за унищожаване на информационни носители*.

Ненадзиравани потребителски устройства

55. Служителите не трябва да оставят оборудване без защита и наблюдение.

56. Всички компютърни конфигурации, когато не са надзиравани, се защитават посредством предпазен екран с парола (password-protected screensaver), т. е. заключване на екрана при 10 минути неактивност, след което посредством logging-on (control-alt-delete) и правилно въвеждане на текущата парола, достъпът се възстановява.

57. Служителите трябва да прекратяват активните сесии, когато приключат работа, трябва да се отписват от приложения и мрежови услуги, когато повече не са им необходими.

58. Компютърните конфигурации и периферните устройства трябва да се изключват в края на работния ден.

Политика за чисто бюро и чист екран

59. Приетата политика за "чисто бюро и чист екран" спомага да се намалят рисковете от неоторизиран достъп, загуба и повреда на информация по време или извън обичайното работно време. Бюрата на служителите трябва да са чисти от хартиени документи и преносими информационни носители. Политика за чист екран включва защитени посредством предпазен екран с парола компютърни конфигурации, когато не са в употреба.

60. Отговорните служители трябва да съхраняват в заключващи се каси, метални шкафове и други сигурни мебели, хартиените и електронните носители, съдържащи чувствителна или критична информация, свързана с дейността, когато не се използва и по-специално в извънработно време.

61. Сигурното съхранение е превантивна мярка за защита на документи и информация от бедствия като пожар, земетресение, наводнение или експлозия.

62. Компютърните конфигурации, на които се обработва чувствителна информация, трябва да са подходящо разположени като се ограничи възможността за наблюдение на екрана.

63. При печатане на документи, съдържащи чувствителна информация, трябва да се използва персоналният принтер или да се печата в защитен режим с парола, така че тези, които са подали документ за печат, да са единствените, които могат да вземат своите копия след като отидат до принтера и въведат паролата.

V. УПРАВЛЕНИЕ НА СМЕНЯЕМИ НОСИТЕЛИ

64. Сменяемите носители (магнитни и оптични дискове, флаш-памети, карти памет и др.) и хартиените документи трябва да се съхраняват в безопасна и сигурна среда с цел предотвратяване на неоторизирано разкриване, изменение, премахване или разрушаване на информацията, съхранявана върху тях.

65. Всички носители на лични данни се съхраняват от отговорните служители в заключващи се каси и шкафове като достъпът до тях е ограничен и контролиран.

66. При предстоящо изнасяне от администрацията на презаписваеми носители, предишното им съдържание, ако не е нужно повече, трябва да се изтрива.

67. Изнасяне на носители извън администрацията се разрешава единствено във връзка с изпълнение на преките задължения като опаковката им трябва да е подходяща, вкл. папка, джоб, плик.

68. По време на транспортиране, носителите, съдържащи чувствителна информация, трябва да бъдат защитени срещу неоторизиран достъп, използване не по предназначение или

подправяне, трябва да се използват надежден транспорт и куриери, а опаковката трябва да осигурява достатъчна защита на съдържанието от физически повреди.

69. Специалните мерки за защита от нерегламентирано разкриване или изменение при транспортиране на носителите, съдържащи чувствителна информация, трябва да включват използване на заключени контейнери; доставяне на ръка; запечатана опаковка, която прави видим всеки опит за отваряне; в изключителни случаи, разделяне на пратката на повече части и доставяне и изпращане по различни маршрути; използване на дигитални (цифрови) подписи и шифроване за осигуряване на конфиденциалността.

VI. ЗАЩИТА НА ЗАПИСИТЕ

70. Записите на администрацията трябва да бъдат защитени от изгубване, разрушаване, фалшифициране, неоторизиран достъп или неоторизирано огласяване в съответствие със законовите, регулаторни и договорни изисквания и изискванията за дейността.

71. Записите са класифицирани и подлежат на съхранение при спазване на реда на *Закона за националния архивен фонд*, вътрешните нормативни документи и в съответствие с номенклатурата на делата със срокове за съхраняване.

72. Записите са категоризирани по типове, например: класифицирана информация, записи, съдържащи лични данни, счетоводни записи, записи на бази данни, записи на транзакции, контролни записи и работни процедури, всеки с подробности за периодите на запазване и вида на позволения запаметяващ носител, например хартия, магнитен, оптичен.

73. След изтичане на периода за съхранение на записите, ненужните носители подлежат на унищожаване.

74. Административната информационна система следва да поддържа и осигурява съхранението на записите, на приетите и създавани електронни документи за срок не по-малък от 20 години по начин, позволяващ възпроизвеждане на документите без загуба на данни.

VII. КОНТРОЛ НА ДОСТЪПА

75. Служителите получават възможност за достъп до ресурсите на локалната мрежа на администрацията в домейн **vt-government.local** след влизане с регистрирано потребителско име **ime.familya** в регистриран компютър **OAVT-XXX** и чрез временна парола, която трябва да се промени при първо влизане и после през интервал от 35 дни.

76. Избраните пароли трябва да с минимална дължина поне от осем символа и да съдържат поне по една цифра, специален символ, голяма и малка букви. Не е допустимо повторно използване на поне три предишни пароли.

77. Служителите трябва да пазят в тайна паролите си, да избягват записа им на видно място - на хартия, в явен вид онлайн или в незащитен файл.

78. Забранява се използването на едни и същи пароли за целите на дейността и за други цели.

79. Забранява се на служителите да споделят своите потребителски имена и пароли с трети лица.

80. Паролите трябва да се променят, когато има признак за евентуалното им компрометиране.

81. Всеки служител в съответствие със служебните си задължения получава достъп само до тези активи, информационни системи, приложения и данни, които са необходими за изпълнение на възложените му функции.

82. Конкретните **права за достъп** на потребителите до информационни системи и данни се утвърждават от Областен управител/Главен секретар/Директор на дирекция чрез документ *04 ОД-09.01 Права за достъп на потребителите до системите.* Отнемането на правата за достъп до системите при напускане или промяна в назначението се регистрира в същия документ.

83. Служителите носят дисциплинарна отговорност, ако се установи, че чрез предоставените им потребителски имена и пароли използват неправомерно ресурсите на компютърната мрежа, както и че извършват действия, които улесняват трети лица за несанкциониран достъп.

84. За **сигурно влизане** в системи като търговския регистър, регистъра на обществените поръчки, порталите с услуги на НАП и НОИ, електронното банкиране, където се изисква силна автентификация и верификация на идентичността, се използват сертификати за електронен подпис.

VIII. СИГУРНОСТ НА РАБОТАТА

85. Забранено е използването на нерегламентиран софтуер, на софтуер, който е само за лична употреба, и софтуер, чийто произход по отношение на това дали е потенциално злонамерен, е неизвестен или подозрителен. Неконтролираното инсталиране на софтуер на компютърни устройства може да доведе до въвеждане на уязвимост и оттам до изтичане на информация, загуба на цялостност или други инциденти със сигурността на информацията, или до нарушаване на правата на интелектуална собственост.

86. Служителите трябва да използват софтуер само от "белия списък", одобрен от Областния управител и документиран в **Приложение 3** *Списък на използваните приложения*. Инсталиране на софтуера се извършва само от СМИС или под негов контрол.

87. СМИС изготвя инструкции/процедури за работа със системите (**Приложение 4**).

88. На компютърните конфигурации на служителите се инсталират поддържат само версии на използвания в системите им софтуер, които се поддържат от техните доставчици или производители и са актуални от гледна точка на сигурността.

89. Защитата от зловреден софтуер се поддържа в актуално състояние, за да има способността да защитава от новооткрити заплахи; да позволява извършване на пълна проверка за наличие на зловреден софтуер; да позволява извършване проверка на електронната поща и файлове, свалени от интернет, както и преносими записващи устройства, преди да бъдат отворени.

90. Защита от злонамерен софтуер на всички сървъри и компютърни конфигурации се извършва чрез WEB базиран софтуер Bitdefender, който постоянно се актуализира.

91. Интегрирана защита на интернет трафика от различни заплахи, вкл. чрез уеб филтриране на съдържанието, антиспам, антивирусна, антиспайуер защита, се осъществява чрез FortiGate 60D

92. При поява на съобщение от антивирусната програма за опасност от злонамерен код, всеки служител задължително информира СМИС.

93. Преди да се използват, всички файлове на преносими записващи устройства, на електронни и оптични носители с неясен произход или получени по електронна поща и несигурни мрежи, трябва да се проверяват за злонамерен софтуер.

94. При всяко съмнение за наличие на зловреден софтуер като необичайно съобщение, съдържащо неразбираеми знаци, разширение на приложен файл .exe, .vbs, .reg и архивни файлове и др., които могат да предизвикат промени в системната конфигурация, незабавно се уведомява СМИС.

95. На служителите, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици) се забранява: да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга); да ги използват извън рамките на служебните си задължения; да ги предоставят на външни лица без да е заявена услуга. За нарушение целостта на данните се считат действия като унищожаване на бази данни или части от тях; повреждане на бази данни или части от тях; вписване на невярна информация в бази данни или части от тях.

96. Забранено е съхраняването на лични файлове с текст, изображения, видео и аудио на сървърите на администрацията.

97. СМИС осигурява създаване на резервни копия по график на определени, критични за дейността информационни системи, данни и документи.

IX. СИГУРНОСТ НА КОМУНИКАЦИИТЕ

98. Администрацията има мрежова свързаност с административните структури чрез Единната електронна съобщителна мрежа (ЕЕСМ) на държавната администрация и за нуждите

на националната сигурност, интегрирана мрежа за пренос едновременно на данни, глас и видео с гарантирано качество.

99. Локалната мрежа на администрацията е в домейн ***vt-government.local*** като мрежовите ресурси се управляват чрез Active Directory Domain Services, DNS Server, DHCP Server.

100. Вътрешната електронна комуникация се осъществява чрез използване на споделени ресурси в рамките на локалната мрежа на администрацията при регламентирани права на достъп за всеки потребител.

101. При прекъсване достъпа до споделения ресурс, всеки потребител трябва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация. При възстановяване на достъпа, всички локално запазени файлове следва да се преместят отново на сървъра и да се изтрият локалните копия.

102. Интернет се доставя за локалната мрежа на администрацията и за разделената от нея **безжична мрежа GovVT**.

103. При необходимост от дистанционен достъп трябва да се използват само високо надеждни SSL връзки и/или VPN комуникации. Забранено е използването на Icq, Skype, TeamViewer и др., осигуряващи достъп на компютрите извън рамките на локалната мрежа на администрацията и създаващи предпоставки за идентифициране на IP адресите им и за достъп на злонамерен софтуер.

104. При обмен на информация с клиенти и други административни структури се използват различни средства за комуникация: Среда за електронен обмен на съобщения (СЕОС), Модул за електронно връчване (е-Връчване), Среда за междурегистров обмен на данни (RegiX), електронна поща, лицензиран пощенски оператор, телефон, видео, форма за обратна връзка на интернет страницата и др.

105. Служителите в администрацията трябва да използват за получаване и изпращане на официална служебна кореспонденция в електронен вид единствено официалния имейл на администрацията governor@velikotarnovo.government.bg (governor.veliko.tarnovo@gmail.com).

106. Служителите не могат да използват за получаване и изпращане на служебна кореспонденция друга, освен служебна поща **ime.familia@velikotarnovo.government.bg**. Подробна информация за служебната поща може да се намери в **Приложение 4** *Инструкции/процедури за работа със системите (1) Инструкция за ползване на служебни електронни пощенски кутии*.

107. Отговорност на служителите при комуникация е да не излагат на риск администрацията, например чрез клевета; тормоз посредством електронна поща или телефон, било то посредством говор, честота на повтаряне или размер на съобщенията; подмяна на самоличност; изпращане на материали към реципиенти, които изрично не са заявили такива материали (спам); изготвяне и обявяване на лъжливи обяви или услуги от името на администрацията; поемане явно или косвено на задължения или ангажименти към трети лица, ако те не са част от нормалния процес на работа; използване на електронни съобщения за нерегламентирано разпространение на оферти, реклама, предлагане на услуги и др. в полза на други организации; използване устройства на администрацията за нерегламентирана агитация, разпространение на порнографски и други забранени от закона материали; неоторизирани покупки и т.н.

108. Служителите не трябва да водят поверителни разговори на обществени места или по несигурни комуникационни канали, при отворени офиси и места за среща.

X. ДОКЛАДВАНЕ ЗА СЪБИТИЯ И СЛАБОСТИ В СИГУРНОСТТА

109. Всеки служител, възможно най-бързо, трябва да докладва за събития със сигурността на информацията, за всяка наблюдавана или предполагаема слабост в сигурността на системите, услугите и устройствата, вкл. мобилните.

110. Процедурата за докладване на събитие или слабост със сигурността на информацията стартира като служителят веднага уведомява прекия си ръководител и ССИ, попълва *04 ОД-16.01 Доклад за събитие или слабост, свързани със сигурността на информацията* и го предава незабавно на Областния управител и/или на ССИ и ССИС.

111. Случаите, които да бъдат взети под внимание за докладване на събития със

сигурността на информацията, включват: а) неефикасен контрол на сигурността; б) нарушаване на очакванията за цялостност, поверителност или наличност на информацията; в) човешки грешки; г) несъответствие с политики или указания; д) нарушения на организацията на физическата сигурност; е) неконтролирани изменения на системата; ж) неправилна работа на софтуер или хардуер; з) нарушения на достъпа.

112. При загуба на данни или информация от служебния компютър, служителят незабавно докладва за събитието и същевременно уведомява СМИС, който да му окаже съответна техническа помощ.

113. Служителите и доставчиците не трябва да правят опити да доказват подозрителни слабости в сигурността. Изпитването на слабостите може да се тълкува като потенциална злоупотреба със системата, може да причини повреда на информационната система и да доведе до правна отговорност за лицето, което извършва изпитването.

114. Всички служители в администрацията трябва да преминат обучение за действия при инциденти с мрежовата и информационна сигурност.

115. Докладваните събития и слабости в сигурността се оценяват и тогава следва решението дали да се класифицират като инциденти със сигурността.

116. Първоначалната реакция на инцидент със сигурността на информацията е системата да се върне на приемливо ниво на сигурност, след което да се пристъпи към възстановяване на неблагоприятните последици от инцидента и на финала – пълно възстановяване дейността на системата.

XI. УЯЗВИМОСТИ, ЗАПЛАХИ, РИСКОВЕ ЗА СИГУРНОСТТА

117. Администрацията оценява и третира рисковете за сигурността, които се определят като фактическо състояние, което създава заплахи за уязвяване на един или няколко информационни актива, което да предизвика тяхното повреждане или унищожаване.

118. Заплахите имат потенциала да навредят на активи като информация, процеси и системи и по този начин на администрацията. Заплахите могат да имат природен или човешки произход и могат да бъдат случайни или преднамерени.

119. Уязвимостите са слабост на актив или на група активи, която може да бъде използвана от една или повече заплахи. Уязвимости може да се идентифицират в следните области: организация; процеси и процедури; управленски практики; персонал; физическа среда; конфигурация на информационната система; хардуер, софтуер или комуникационни устройства; зависимост от външни страни.

120. Служителите трябва своевременно да съобщават за забелязани от тях уязвимости/заплахи чрез **Приложение 5** *Анкета за уязвимости/заплахи, свързани със сигурността на информацията* като обобщената информация се взема предвид при оценяване на риска.

121. Информацията за техническа уязвимост на използваните информационни системи трябва да бъде получена навреме. В зависимост от това, колко спешно трябва да се обърне внимание на техническата уязвимост, се предприемат действия според механизмите за контрол, свързани с управлението на изменения или чрез следване на процедурите за реакция на инцидент със сигурността на информацията. Процесът на управление на техническите уязвимости се наблюдава и оценява, за да се осигури неговата ефикасност и ефективност като първо се обръща внимание на системите с висок риск.

122. Сканирането на мрежови портове или за уязвимости е строго забранено, ако преди това не е уведомен СМИС.

XII. СЪОТВЕТСТВИЕ СЪС ЗАКОНОВИ И ДОГОВОРНИ ИЗИСКВАНИЯ

123. Администрацията използва само операционни системи, приложен софтуер, информационни системи и продукти, които са в съответствие с правата на интелектуална собственост.

124. Служителите трябва да познават нормативните изисквания, свързани със защита на правата по силата на закон (лични данни, авторски права), търговска тайна, патенти и др. и да ги спазват, като за допуснати нарушения може да се носи дисциплинарна отговорност.

125. Върху компютърните конфигурации и сървърите се инсталират само софтуерни продукти, за които администрацията разполага с лиценз.

126. Строго е забранено копирането, изцяло или частично, на фотографии, статии, музика, филми, книги и други, без упълномощаване от собственика на материала, защитен с авторски права.

127. Администрацията осигурява поверителност и защита на информацията за самоличността в качеството си на регистриран администратор на лични данни по смисъла на Закона за защита на личните данни и е определила регистрите с лични данни, които поддържа.

128. Прилагането на необходимите организационни мерки за защита на личните данни се осъществява от служителите на ръководни длъжности в администрацията и от конкретните служители, оторизирани да обработват лични данни.

129. При публикуване на документи на интернет страницата на администрацията, личните данни, съгласно Регламент (ЕС) 2016/679 защита на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни се заличават и на тяхно място се добавя следния текст: „Заличени лични данни, съгласно Регламент (ЕС) 2016/679“.

Приложения:

Приложение 1 *Протокол за предаване на информационни активи*
Приложение 2 *Инструктаж за обезпечаване сигурността на оборудването извън инфраструктурата на Областна администрация Велико Търново*
Приложение 3 *Списък на използваните приложения*
Приложение 4 *Инструкции/процедури за работа със системите*
Приложение 5 *Анкета за уязвимости/заплахи, свързани със сигурността на информацията*