КЛАСИФИКАЦИЯ: [НИВО 1] TLP:GREEN

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

Вътрешни правила за администрирането, експлоатацията и поддръжката на хардуер и софтуер

I. ОБЩИ ПОЛОЖЕНИЯ

1. Настоящите вътрешни правила са разработени на основание чл. 5, ал. 1, т. 6, във връзка с чл. 14, чл. 16, чл. 17, чл. 19, чл. 20, чл. 21, чл. 22, чл. 23, чл. 24, чл. 25, чл. 28, чл. 29, чл. 32 и чл. 33 от Наредбата за минималните изисквания за мрежова и информационна сигурност (Наредбата).

II. СИГУРНОСТ НА МРЕЖИТЕ И КОМУНИКАЦИИТЕ

Управление на сигурността на мрежите

1. Локалната мрежа на администрацията е съставена от присъединени към домейн **vt-government.local** компютърни системи.

2. Поддържа се мрежа за безжичен интернет достъп **GovVT**.

3. Осигурена е свързаност на администрацията с Единната електронна съобщителна мрежа (ЕЕСМ) на държавната администрация и за нуждите на националната сигурност, чрез която се осъществява: мрежова свързаност с централизирани ресурси; централизирана защита на информационните ресурси, свързани в мрежата; достъпност до ресурсите в мрежата; интегритет на данните и информацията в мрежата; пренос на данни, глас и видео с гарантирано качество.

4. Мрежовите ресурси на локалната мрежа в домейн **vt-government.local** се управляват чрез Active Directory Domain Services, DNS Server, DHCP Server.

5. Интернет страницата и електронните пощенски кутии на администрацията са локализирани на централизирана инфраструктура на държавната администрация:

5.1 Официална интернет страница – https://vt.government.bg;

5.2 Официална електронна поща: governor@velikotarnovo.government.bg

5.3 Служебна персонална електронна поща: ime.familia@ velikotarnovo.government.bg

6. Използването на пощенски платформи на трети страни за служебни цели може да е рисково и да доведе до разкриване на държавна, конфиденциална или лична идентифицираща информация (по смисъла на ЗЗЛД). Публичните/безплатни имейл платформи като mail.bg, abv.bg, vip.bg, yahoo.com, outlook.com, gmail.com, mbox.contact.bg, orbitel.bg и др. не гарантират конфиденциалност на данните, съхранявани в пощенските кутии.

7. Защита на мрежата може да се реализира посредством забрана на приложения чрез защитната стена, за да се предотвратят събития за влизане от необичайни места, включително TOR мрежи, приложения за чат като Trello и Discord и др.

8. Дейностите по администрирането, експлоатацията и поддръжката на мрежите и системите се извършват в съответствие с утвърдени *Инструкции/процедури/насоки за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер* (**Приложение 1**).

9. За защита на услугите и приложенията от неоторизиран достъп се използват механизми за контрол като квалифициран електронен подпис, сървърен сертификат, механизми за управление на достъпа, механизми за идентификация, филтриране на интернет трафика, забрана на ненужни портове и др.

10. Правата за достъп до мрежата, компютърните конфигурации, информационните системи, данните и приложенията се регламентират стриктно чрез определянето и оторизирането им в *Права за достъп на потребителите*.

11. Информация за извършено инсталиране и настройки на сървърите и компютърната техника както и за извършените изменения се съдържа в картата на всеки актив *Карта на информационни ресурси* (**Приложение 2).**

12. Информация за повреди, изменения, грешки и събития, свързани със сигурността се отразяват в *Регистър на събитията, свързани със сигурността на информацията*.

13. С цел взимане на информирани решения в случай на инцидент със сигурността, се поддържат актуални *Опис на информационните активи* и схемите и документите на мрежовата ИТ инфраструктура: *Физическа схема на свързаност*, *Логическа схема на информационните потоци* **(Приложение 3)**, *Документация на структурната кабелна система*, *Матрица за резервиране и архивиране на информацията* **(Приложение 4)**, *Техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти*.

Защита на хардуерни устройства

14. За намаляване на риска от инциденти, предизвикани от технически повреди, администрацията:

14.1 осигурява климатико-механичните условия, указани от производителя;

14.2 осъществява наблюдение на параметрите на климатико-механичните условия в сървърното помещение;

14.3 провежда периодично техническа профилактика.

Сървърно помещение

15. Сървърното помещение осигурява оптимална, безопасна и стабилна работа на комплекс от оборудване (сървъри, комутатори, дисков масив, непрекъсваемо електрозахранване, монтирани в сървърен шкаф), което изпълнява основни процеси в администрацията.

16. Осигуряването на подходящи условия за хардуера, увеличава надеждността и продължителността му на живот:

16.1 оптималната температура за правилното функциониране на активното оборудване е в диапазона от 18 до 24 градуса по Целзий, за което е необходимо да се използва климатик, който да работи непрекъснато и денонощно, да осигурява зададения температурен режим както през лятото, така и през зимата;

16.2 относителната влажност трябва да се поддържа в диапазона от 30 до 55 %.

17. Сървърното помещение трябва да е оборудвано с противопожарна инсталация и с ключалка на входната врата, гарантираща достъп само на оторизиран персонал.

Защита на DNS и УЕБ сървъри

18. За защита на Domain Name System (DNS) следва да се предприемат следните мерки:

18.1 прилагане DNSSEC (Domain Name System Security Extensions);

18.2 минимизиране DNS заявките съгласно RFC 7816 на IETF от 2016 г.;

18.3 забрана на zone-transfers, тъй като злонамерени лица могат бързо да определят всички хостове в определена зона чрез трансфери на DNS зони, да събират информация за домейна, да избират цели за атаки, да откриват неизползвани IP адреси и да заобикалят мрежовия контрол на достъпа, за да крадат информация.

19. За защита на уеб сървъри следва да се предприемат следните мерки:

19.1 инсталиране сертификат на уеб сървърите, издаден от доверена система за сертифициране (trusted certification authority system);

19.2 за защита интегритета на информацията, обменяна с потребителите, уеб сайтът (website) трябва да е достъпен само по протокол Hypertext Transfer Protocol Secure (HTTPS);

19.3 възможност за криптиране на информацията, обменяна между уеб сървъра и потребителите му;

19.4 не се позволява вмъкване на данни от страна на потребителя, освен на определените за това места;

19.5 за защита от brute force атаки да се въведе ограничение на броя неуспешни опити за влизане в системата.

Обмен на информация

20. За получаване и изпращане на електронни документи и съобщения между администрациите приоритетно се използва Средата за извършване на електронен обмен на съобщения (СЕОС).

21. Системата за сигурно електронно връчване (ССЕВ) се използва приоритетно за обмен на документи с физическите и юридически лица, регистрирани в системата, както и с администрациите при необходимост.

22. Като резервен канал за обмен на електронни документи и съобщения се използва официалната електронна поща на администрацията governor@velikotarnovo.government.bg.

23. Служителите обменят оперативна служебна информация чрез персоналната си служебна електронна поща ime.familia@velikotarnovo.government.bg.

24. Служителите обменят информация във вътрешната компютърна мрежа посредством осигурен персонален достъп с акаунт **ime.familia** като използват информационни системи и споделени папки.

Защита на информацията при отдалечен достъп/работа от разстояние

25. Политиката се отнася за всички, за които се осигурява отдалечен достъп до информационните ресурси на администрацията – служители, доставчици на услуги по поддръжка на информационната и комуникационна инфраструктура и системи.

26. Заявяването и предоставянето на достъп за работа от разстояние на служител или доставчик се осъществява като се следват договорните изисквания и политиките за управление на достъпа и за автентикация.

27. При необходимост от достъп до информационните системи на администрацията или до информационни системи извън мрежата, контролирана от администрацията, трябва да се използват канали с висока степен на защита като Virtual Private Network (VPN) и най-малко двуфакторна автентикация.

28. При работа от разстояние не трябва да се използват File Transfer Protocol (FTP) и Remote Desktop Connection.

29. При работа от разстояние трябва да се използва надеждна интернет връзка, като за безжичен достъп се изисква да се използва протокол WPA2.

30. За дистанционна работа трябва да се използват служебни преносими компютри (лаптопи), с приложени политики и правила за защита и логически достъп.

31. При използване на лични технически средства за работа от разстояние се прилагат технически мерки за защита като задължително се създава отделен профил за достъп до компютърната конфигурация.

32. Забранява се свалянето и съхранението на данни с категория „Ниво 1“, „Ниво 2“ и „Ниво 3“ локално на личен хардуер при работа от разстояние.

33. Обработването на информация трябва да се извършва само на сървъри на администрацията.

34. При необходимост от дистанционна работа, на потребителя може да се определи времеви диапазон за достъп до информационните ресурси.

35. Не се допуска запаметяване на данните за удостоверяване при свързване през VPN.

36. Всички логове на работещите от разстояние се съхраняват минимум 1 година.

37. Всички стационарни и мобилни компютри, които се свързват от разстояние, трябва да бъдат защитени с антивирусни програми.

38. Дисковете на мобилните компютри, които се използват за дистанционна работа, за целта трябва да бъдат с включен BitLocker.

Филтриране на трафика

39. Трафикът между отделните системи и техните подсистеми се контролира чрез подходящо филтриране (по IP адрес, по протокол, по номер на порт от Transmission Control Protocol (TCP)/Internet Protocol (IP) стека и т. н.) с цел превенция на евентуални атаки и ограничаване на разпространението на инциденти.

40. Редовно трябва да се прави преглед на отворените портове (например чрез https://www.shodan.io), защото някои фамилии зловреден софтуер отварят „задни вратички“, през които се имплементират други зловредни софтуери. Особено внимание да се обърне на затварянето на портовете на популярни услуги, като например 25 и 21.

41. Ненужните портове по протоколи TCP и User Datagram Protocol (UDP) трябва да се забраняват чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика.

42. Ако се установят ненужни услуги (services) на сървърите, те трябва да се спрат и да се блокират, а не да се филтрират портовете, които не се използват.

Периодично трябва да се преглеждат услугите на сървърите

43. Администрацията трябва да поддържа актуален списък на услугите, които се предлагат чрез ИТ инфраструктура на администрацията като за всяка услуга има следната информация:

43.1 кои информационни активи участват в предоставянето й;

43.2 с кои други услуги е обвързана;

43.3 откъде трябва да се достъпват - локална мрежа и/или интернет;

43.4 какъв е достъпът до нея - свободен или контролиран достъп на потребителите;

43.5 кой отговаря за нея;

43.6 кой я администрира;

43.7 какъв е приоритетът на услугата, от гледна точка на оперативната дейност, на имиджа и на финансовите резултати на администрацията, за да може в случай на инцидент бързо да се прецени, кои услуги ще бъдат засегнати и кои може да бъдат спрени.

III. СИГУРНОСТ НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ

Използване и защита на софтуер и фърмуер

44. Софтуерът и фърмуерът се инсталират само от СМИС или след съгласуване с него - от доставчици на информационни системи, които имат администраторски акаунт.

45. СМИС инсталира и поддържа само версии на използвания софтуер и фърмуер, които се поддържат от техните доставчици или производители и са актуални от гледна точка на сигурността.

46. Всички операционни системи, бази данни, приложения, защитни стени и прилежаща инфраструктура, трябва да бъдат настроени за регулярни обновления за „кръпки“ и „поправки“ за уязвимости, разпространявани от производителя.

47. СМИС редовно следи за новооткрити уязвимости в сигурността на използвания в системите софтуер и фърмуер и за инсталиране на техните актуализации (нови версии, ъпдейти и пачове), които отстраняват тези уязвимости, или мерки за смекчаването им, публикувани от производителите или доставчиците.

48. На сървърите и компютърните конфигурации на администрацията се **забранява** инсталиране и използване на **неоторизиран** софтуер, софтуер, който е само за лична употреба, и софтуер, чийто произход по отношение на това дали е потенциално злонамерен, е неизвестен или подозрителен.

49. Софтуер се инсталира само ако е одобрен в *Списъка на одобрения софтуер, който се използва в информационните и комуникационните системи (Бял списък).* Друг софтуер се инсталира след заявяване, потвърждаване на необходимостта от него и одобряването му в Белия списък.

50. При спрян от поддръжка софтуер, СМИС своевременно планира и предлага включване на миграция към нови версии в годишния план на необходимите ресурси.

51. СМИС поддържа библиотека с дистрибутиви на използвания софтуер и фърмуер в актуално състояние с цел намаляване на времето за възстановяване на дадена система след срив. СМИС управлява достъпа до нея.

52. Достъп до библиотеката с дистрибутиви на софтуер на Майкрософт е осигурен чрез Информационна система за лицензите в администрацията (ИСЛА) – msoft.goverment.bg с потребителско име и парола за оторизиран служител. СМИС е отговорен за поддържане на акаунта.

Изисквания за сигурност при конфигуриране на системи и приложения

53. При инсталиране и конфигуриране трябва да се прилагат препоръките за сигурност на съответния доставчик или производител.

54. СМИС конфигурира по подразбиране, а потребителите се уведомяват да спазват следните изисквания:

54.1 забрана на macros в office пакетите, с изключение на времето, в което се работи по служебни документи;

54.2 забрана на pop-up в браузерите, с изключение на времето, в което се работи служебно със системи;

54.3 Auto play функцията винаги да иска потвърждение на потребителя;

54.4 най-високо ниво на User Account Control, за да се издава винаги предупреждение;

54.5 забрана на AutoComplete;

54.6 блокиране на рекламно съдържание чрез приложения (add-ons) към браузърите.

55. СМИС трябва да спазва следните изисквания при конфигуриране:

55.1 при споделяне на файлове и принтери да не се използва настройка Everyone, а да се указва точно кои акаунти да имат право на достъп;

55.2 забрана на TRACE/TRACK методът;

55.3 забрана на anonymous authentication;

55.4 използване на Unicast Reverse-Path Forwarding (uRPF) за предпазване от използването на фалшиви IP адреси и rate-limiting за ограничаване броя на заявките по IP адрес;

55.5 забрана на TLS renegotiation в системи, използващи TLS, или конфигуриране rate-limiter за ограничаване броя на предоговаряне на сесия;

55.6 съобщенията за грешки в системите да не дават излишна информация.

56. СМИС трябва да забрани достъпът до BIOS, да постави парола на всяка компютърна конфигурация. В BIOS трябва да се забрани зареждане на операционна система (boot) от всяко друго устройство, освен от твърдия диск на компютъра.

Защита от злонамерен софтуер

57. Защитата от злонамерен софтуер в информационните системи на администрацията е ориентирана в две основни направления: забрана за използване на нерегламентиран софтуер и задължително използване на утвърден за цялата администрация антивирусен софтуер.

58. Защита от злонамерен софтуер на всички сървъри и работни станции се извършва чрез WEB базиран софтуер **Bitdefender**, който постоянно се актуализира.

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

60. Администрацията ползва услугите на CERT Bulgaria или Националния център за действие при инциденти в информационната сигурност за извършването на проактивни дейности за намаляване рисковете от инциденти в компютърната сигурност и при разрешаването на такива инциденти в случай, че вече са възникнали.

61. На сървърите и на компютърните конфигурации на служителите се инсталира само оторизиран софтуер, този от *Списъка на използваните приложения* (Белия списък).

62. СМИС следи да се спазва забраната за инсталиране 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.

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

64. Подготовката за предпазване от *Ransomware и/или унищожаване на данни* включва: Актуализиране на архивите и задължителното им съхраняване в офлайн копие, така че зловреден код да не може да ги компрометира, дори и цялата мрежа да е засегната. Тестването на плановете за архивиране и възстановяване е от решаващо значение.

65. Подготовката за предпазване от *DDoS атака* включва: Консултиране се с доставчиците на достъп до Интернет какви контрамерки са предприели или могат да предприемат срещу евентуални DDoS атаки.

Процедури за сигурно влизане в системите

66. За сигурно влизане в локалната мрежа, информационните системи и данни, за доказване на идентичността и автентификация, потребителите използват качествени пароли.

67. За сигурно влизане в централизирани уеб базирани системи като регистри и системи на електронното управление, порталите с услуги на НАП, НОИ, системи за разплащане и др., където се изисква силна автентификация и верификация на идентичността, се използва удостоверяване на квалифициран електронен подпис.

68. При влизане трябва да се разкрива минимално количество информация за системите или приложенията, с цел да се избегне предоставянето на ненужна помощ на неоторизиран потребител.

Използване на криптографски механизми за контрол

69. Криптографските механизми трябва да гарантират конфиденциалността и интегритета на чувствителната информация в съответствие с нейната класификация.

70. Администрацията прилага криптографски механизми за защита на чувствителната информация, идентифицирана в *Списък и класификация на чувствителната информация и ресурси, в съответствие с нейната класификация*, за гарантиране на конфиденциалността и интегритета й.

71. Достъпите на служителите до централизираните информационни системи са определени със заповеди и се осъществяват посредством квалифициран електронен подпис (КЕП). В *Списъка на издадените удостоверения за електронен подпис* се поддържа информация за валидните КЕП и съответните системи, които се достъпват чрез КЕП.

IV. УПРАВЛЕНИЕ НА ДОСТЪПА

72. Ръководството на администрацията разрешава достъп до информационните и комуникационни системи на администрацията на потребител или автоматизиран процес само когато този достъп е строго необходим на потребителя, за да изпълни задълженията си, или на автоматизирания процес, за да извърши необходимите технически операции.

73. За да гарантира, че достъп до информационните и комуникационните системи имат само оторизирани потребители, устройства (включително други информационни системи) и автоматизирани процеси, ръководството:

73.1 определя правата на достъп до конкретни информационни активи на служителите според длъжността им;

73.2 определя реда за заявяване, промяна и прекратяване на достъп;

73.3 прилага задължителни мерки за автентикация, оторизация и одит на компютърните мрежи и системи;

73.4 гарантира, че потребителските профили са индивидуални;

73.5 в ежедневната работа осигурява използване на профили с най-ниското ниво на достъп, което дава възможност за изпълнение на служебните задължения;

73.6 гарантира редовни прегледи на достъпите, не по-рядко от веднъж в годината;

73.7 ограничава даването на привилегирован достъп като този достъп се дава по изключение на служители за изпълнение на определени задължения, само за определен период и действията с него се контролират;

73.8 гарантира, че достъпът до споделени файлове и принтери е разрешен само от локалната мрежа на администрацията.

74. Правата за достъп за служители и доставчици се определят на принципа да са достатъчни за изпълнение на задълженията, без това да нарушава сигурността на

данните в зависимост от тяхната поверителност.

75. Всеки служител на администрацията има точно определени права на достъп и използва индивидуален потребителски профил за вход в системите и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран.

76. Не е разрешено използването на групови профили.

77. Всеки служител в съответствие със заеманата длъжност получава достъп само до тези активи, информационни системи, приложения и данни, които са необходими за изпълнение на служебните задължения.

78. Правата за достъп на доставчиците (трети страни) се определят съгласно предмета на дейност в сключените договори.

79. Не се задава и не се осигурява достъп на неоторизирани лица.

80. Създават се два типа акаунти: администраторски и потребителски. Администраторски акаунт се осигурява на служител или доставчик, който извършва операции като инсталиране, конфигуриране, управление, поддръжка. На всички останали служители се предоставя потребителски акаунти.

81. Всички акаунти са персонални за служителите на администрацията и за служителите на доставчиците.

82. Не се разрешава да се ползва чужд акаунт за достъп до информационни системи и ресурси.

83. Управлението на потребителите, техните привилегии и автентикации в локалната мрежа от домейн **vt-government.local** се извършва чрез Active Directory Domain Services и др. от операционна система Windows Server.

84. Конкретните права на достъп до информационните системи, данните и приложенията се документират стриктно в документ *Права за достъп на потребителите*, който се утвърждава от областния управител, главния секретар или директорите на дирекции.

Заявяване на достъп

85. Заявяване на достъпа за новопостъпил служител до локалната мрежа и информационните системи и данни на администрацията се стартира от служител „Човешки ресурси“, който уведомява прекия ръководител за назначението. Необходимата информация включва:

- Имената на служителя;
- Длъжност;
- Структурно звено;
- Дата на назначаване.

86. Прекият ръководител (областният управител, главният секретар или директорите на дирекции) заявява до СМИС осигуряване на права за достъп до системите и необходимата компютърна техника и периферни устройства, които ще се ползват от служителя.

Осигуряване достъп на новопостъпил служител

87. Заявеният от прекия ръководител достъп за новопостъпилия служител СМИС документира в *Права за достъп на потребителите* осигурения достъп до

информационните системи и ресурси.

88. След утвърждаването на документа *Права за достъп на потребителите* от прекия ръководител (областния управител, главния секретар или директора на съответната дирекция), документът се подписва от новоназначения служител, с което се удостоверява, че разбира условията на предоставения му достъп.

89. СМИС създава акаунт на служителя за домейн мрежата и за служебна електронна пощенска кутия, осигурява съответните достъпи до информационните системи и ресурси. При създаване на потребителското име се прилага следната конвенция: напр. Иван Димитров – ivan.dimitrov (име и фамилия). При наличие на повторение на име и фамилия, се добавя и инициала от презимето, напр.: Иван Стоянов Димитров – ivan.s.dimitrov.

90. СМИС предоставя на служителя потребителско име и временна парола за достъп както за домейн мрежата, така и за служебната електронна пощенска кутия. Паролата задължително се променя при първоначално влизане от служителя.

91. СМИС осигурява и предава на новия служител необходимото ИТ оборудване като приемането от служителя се документира с *Протокол за предаване на информационни активи.*

92. СМИС инсталира и/или конфигурира ИТ оборудването, като процесът се документира в Приложение X *Карта на информационни ресурси*.

93. СМИС уведомява съответния ръководител за осигурения достъп.

94. СМИС запознава служителя с ИТ оборудването, информационните системи и допустимото им използване.

95. Всички подписани оригинали на *Права за достъп на потребителите, Заявки за даване/прекратяване на достъп* и *Протоколи за предаване на информационни активи* се съхраняват от СМИС.

Промяна правата на достъп

96. Промяна на правата за достъп се извършва в случаите на необходимост от разширяване на правата на достъп или при преместване на друга позиция.

97. В тези случаи се прилага процедурата за *Заявяване на достъп.*

98. Изготвя се нов документ *Права за достъп на потребителите,* а

99. След утвърждаването на документа *Права за достъп на потребителите* от прекия ръководител (областния управител, главния секретар или директора на съответната дирекция), СМИС осигурява съответните достъпи до информационните системи и ресурси.

100. Върху предишния документ *Права за достъп на потребителите* се отбелязва ☑ Промяна права за достъп на потребителя с нов документ 04 ОД-09.01 Права за достъп на потребителите до системите, записва се датата, полагат се подписите на инициирал (служител ЧР), провел (СМИС) и проверил (прекия ръководител).

Прекратяване правата на достъп

101. Прекратяването на правата на достъп се инициира от служител

„Човешки ресурси“, който уведомява прекия ръководител за освобождаването на служителя.

102. Прекият ръководител заявява до СМИС отнемане на предоставената компютърна техника и периферни устройства на служителя, както и прекратяване на достъпа му до информационни ресурси.

103. СМИС приема ИТ оборудването на освободения служител като документира действието с подпис и отбелязване на датата в *Протокола за предаване на информационни активи*.

104. СМИС деактивира акаунта на служителя и съответните достъпи до информационните системи и ресурси.

105. В документ *Права за достъп на потребителите* се отбелязва ☑ Отнемане права за достъп на потребителя, записва се датата, полагат подписите на инициирал (служител ЧР), провел (СМИС) и проверил (прекия ръководител).

Преглед на правата за достъп

106. Преглед правата на достъп се извършва най-малко веднъж годишно.

107. Прегледът на правата на достъп на потребителите включва всички достъпи до системите и ресурсите, описани в документа *Права за достъп на потребителите*.

108. Преглеждат се конфигурациите на системи като Active Directory Domain Services, защитни стени, VPN системи.

109. Преглеждат се достъпите като се следи да се спазва принципа за *минимизиране предоставените достъпи до най-малката нужна привилегия*. Особено внимание трябва да се обърне на привилегированите (администраторски) достъпи.

110. Прегледът се инициира от директорите на дирекции и се възлага от областния управител.

111. СМИС и администраторите на съответните информационни и комуникационни системи предоставят на оправомощените лица списък на всички, които имат достъп до системите и нивото на достъпа.

112. Контролът на предоставените/ограничени права включва следното:

112.1 преглед на предоставените достъпи: дали всички, на които е даден достъп до мрежата, до отделните системи, приложения или данни, имат право на него;

112.2 дали външни лица (бивши служители, представители на трети страни) имат достъп и какъв е той, например за четене, писане, изтриване и изпълнение;

112.3 оправомощените лица от ръководството документирано потвърждават, дават указания за промяна или възлагат прекратяване на тези, които вече не са нужни.

113. СМИС коригира правата и ги актуализира в документа *Права за достъп на потребителите*.

114. Прегледът на акаунтите и достъпите на доставчиците се извършва от

определения за отговорен служител по съответния договор, съгласно политиката за управление на взаимоотношенията с трети страни.

Защита на профилите с административни права

115. **При администриране на информационните и комуникационните системи се** прилагат следните мерки за защита на профилите с административни права:

115.1 преди въвеждане в експлоатация задължително се сменят идентификационните данни на администратора, въведени по подразбиране или инсталирани от производителя/доставчика на информационния актив;

115.2 администраторските профили са персонални;

115.3 администраторските профили се използват само за административни цели;

115.4 администраторските профили се създават само на служители, които извършват административни операции (инсталиране, конфигуриране, управление, поддръжка и т. н.);

115.5 правата на всеки администраторски акаунт са ограничени във възможно най-голяма степен до функционалния и техническия периметър на всеки администратор;

115.6 данните за автентикацията на администраторските акаунти: са различни за всяка система; са с възможно най-голяма сложност, позволена от системата или нейния компонент; съхраняват подходящо физически и логически защитени, като достъп до тях имат само оторизирани служители и ръководители.

115.7 поддържа се списък на администраторските профили за информационните и комуникационните системи и техните компоненти;

115.8 при невъзможност на администратор да изпълнява пълноценно функциите си поради обективни причини правата на административния му акаунт се спират за съответния период;

115.9 поне веднъж годишно се прави преглед на администраторските профили с цел удостоверяване на актуалността им.

116. Всички операции, процеси и дейности в информационните и комуникационните системи и техните компоненти, извършени с администраторски права, се документират чрез автоматично регистриране на всички събития (виж **Системни записи (logs)**) като в документацията не се въвеждат и не се съхраняват пароли на административен профил под формата на явен текст или хеш.

IX. УПРАВЛЕНИЕ НА ПАРОЛИТЕ

117. Управлението на паролите за достъп до информационните ресурси се извършва чрез политиките за сигурност на Активната директория. Изключение от правилото са информационни системи, които не са интегрирани с Активната директория и паролите се управляват локално.

118. Всички пароли са категоризирани като чувствителна информация за

администрацията и са класифицирани като „Ниво 3“ според *Списък и класификация на чувствителната информация и ресурси.*

119. За достъп до информационните ресурси, съобразно акаунтите, се използват два вида пароли: потребителски и администраторски.

Управление на потребителски пароли

120. Прилага се групова политика за управление на паролите на всички потребители на Активната директория на администрацията, която включва:

120.1 налагане задължителна автентикация - използване на пароли;

120.2 позволяване на потребителите да променят своите пароли и включва процедура за потвърждаване на паролите, което намалява входните грешки;

120.3 налагане избор на качествени пароли - с минимална дължина от осем символа и да съдържа комбинация от големи и малки букви на латиница, цифри и специални символи;

120.4 налагане потребителите да променят своите пароли при първото влизане;

120.5 налагане въвеждане на парола след 10 минути неактивност;

120.6 налагане редовни изменения на паролите през интервал от 35 дни;

120.7 поддържане запис на поне три предишни пароли за предотвратяване на повторното им използване;

120.8 неизобразяване паролите на екрана при въвеждане.

120.9 съхраняване файловете с пароли отделно от данните за приложната система;

120.10 съхраняване и предаване на пароли в защитена форма.

121. Всеки потребител носи лична отговорност да пази конфиденциалността на паролите, които използва.

122. Паролите са персонални и не се предоставят на други лица.

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

124. С цел служителите да съхраняват паролите в неявна форма, се допуска да се използват софтуерни инструменти за защита на паролите в криптиран вид, например: Dashlane, One password, Key vault, KeePass.

Управление на администраторски пароли

125. Паролите за автентикация на администраторските профили се сменят задължително: най-малко веднъж в годината; при прекратяването на договорните или служебни отношения със служители или трети страни, на които тези данни са били известни; при пробив в мрежовата и информационната сигурност.

126. Администраторските пароли следва да съдържат малки и големи букви на латиница, цифри и специални символи. Дължината на администраторските пароли трябва да е минимум 12 символа.

127. Администраторските пароли трябва да са различни за всяка система.

128. Администраторските пароли се документират от СМИС на хартиен носител, запечатват се в плик, който се съхранява от Областния управител.

VI. РЕЗЕРВИРАНЕ НА ДАННИ И СИСТЕМИ

129. Ръководството на администрацията предприема подходящи и в съответствие с рисковете мерки за резервиране на системи и данни, за да се гарантира нивото на услугите и дейностите, за да се защити интегритета на информацията в случай на инцидент, засягащ нейната достъпност.

130. Върху дисков масив и др. се резервират системи и данни, определени в *Матрица за резервиране и архивиране на информацията*, за да се гарантира, че цялата съществена информация и софтуер могат да бъдат възстановени след злополука или повреда в носителите.

131. За информацията, подлежаща на резервиране и архивиране, се описват следните данни:

131.1 тип на информацията (бази данни, конфигурационни файлове, имиджи на системи и др.), която ще се резервира и/или архивира;

131.2 технологията, която ще се използва за архивиране и резервиране;

131.3 типът на резервиране (частично, пълно и др.);

131.4 периодът на извършване на архивирането и резервирането;

131.5 броят на копията, които ще се правят;

131.6 времето за съхраняване на всяко копие съгласно изискванията на нормативните актове и оценката на риска;

131.7 мястото на съхраняване на всяко копие;

131.8 начинът на защита от неправомерен достъп (физическа и логическа);

131.9 случаите на използване;

131.10 лицето, което дава разрешение за използването.

132. Администрацията изготвя резервни копия:

132.1 ежедневно на административната информационна система МИКСИ;

132.2 ежеседмично на всички финансово счетоводни данни, ТРЗ, данни „Административни правила и данни“.

132.3 ежемесечно на данни „Съдебни дела“, „Наематели“ и др.

133. Административната информационна система МИКСИ следва да поддържа и осигурява съхранението на приетите и създаваните електронни документи за срок не по-малък от 20 години по начин, позволяващ възпроизвеждане на

документите без загуба на данни.

134. Периодът за съхранение на текущата информация е 12 месеца, освен информацията и данните, за които има определен друг срок за съхраняване в Номенклатура на делата със срокове за съхраняване.

135. Всички изисквания за резервиране и архивиране на информацията се определят от собственика на информацията или с неговото одобрение и трябва да бъдат съобразени с времето, за което тя трябва да се възстанови, за да се гарантира необходимото ниво на наличност на услугата.

136. Резервирането и/или архивирането на информацията се извършва от СМИС или под неговото ръководство.

137. При резервирането и/или архивирането на информацията се спазват следните изисквания:

137.1 правят се регулярни копия съобразно риска от загуба на информация и динамиката на изменението й;

137.2 копията на информация се етикетират по начин, указващ еднозначно поне каква е информацията, за коя система, какъв метод е използван за създаване на копието, дата и час;

137.3 копията на чувствителна информация се криптират или поне се защитават с парола;

137.4 копията на информацията се съхраняват на отделна машина и по възможност в друга защитена мрежа;

137.5 едно от копията на критична за дейността информация се съхранява off-line и по възможност в друга сграда или на отдалечено място;

137.6 прави се регулярна проверка на годността на резервните копия, дали те изпълняват целите, за които са създадени, и постига ли се необходимото време за възстановяване.

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

139. Копията с информация трябва да се проверяват за тяхната годност минимум веднъж годишно, като се отчита времето за тяхното възстановяване, съпоставено с допустимото време за прекъсване.

140. Неуспешните тестове за възстановяване на резервните копия се изследват за причините и се избират коригиращи действия.

141. Тестването на резервните копия се извършва в изолирана тестова среда.

142. Записите с резултатите от тестовете се съхраняват 1 година.

143. Резервиране на компоненти на инфраструктурата, в т.ч. на системи и устройства, се предприема в съответствие с рисковете, за да се гарантира нивото на услугите и дейностите.

X. МОНИТОРИНГ

144. Администрацията трябва да наблюдава събития, които могат да повлияят на мрежовата и информационната сигурност на важните за нейната дейност системи, чрез анализ на информационни потоци, протоколи и файлове, преминаващи през ключови устройства.

Системни записи (logs)

145. Автоматично се регистрират всички събития в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, охранителни съоръжения, мрежово оборудване и работни места на администратори се, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи;

146. В системните записи за всяко събитие е отбелязано астрономическото време, когато то е настъпило.

147. Часовниците на всички системи за обработване на информация в администрацията са синхронизирани с източник на данни за точно време чрез домейн контролер сървър в съответствие с изискванията на стандарти БДС ISO 8601-1 и БДС ISO 8601-2 като за синхронизация на часовниците на компоненти на информационните и комуникационните системи трябва да се използва протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010 г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time), или аналогичен.

148. Достъпът до системните записи трябва да е само за четене и да е ограничен само до лица, имащи задължения за наблюдение, за разрешаването на инциденти с мрежовата и информационната сигурност, за разкриването и разследването на тежки престъпления.

149. Системните записи се архивират и съхраняват за период не по-малък от дванадесет месеца.

ПРИЛОЖЕНИЯ

Приложение 1	Инструкции/процедури/насоки за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер
Приложение 2	Карта на информационни ресурси
Приложение 3	Логическа схема на информационните потоци
Приложение 4	Матрица за резервиране и архивиране на информацията