УТВЪРДИЛ: /п/

ДЕЯН ДОЙНОВ

Кмет на Община Сопот

В Ъ Т Р Е Ш Н И П Р А В И Л А

ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОБЩИНА СОПОТ

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите правила имат за цел осигуряването на контрол и управление на работата на информационните системи в Община Сопот. В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал. Компютрите в Община Сопот са свързани в локална мрежа, разположена в административната сграда 1 на Общината, административна сграда 2, административна сграда 3 и административна сграда в село Анево. Програмните продукти и бази данни могат да бъдат специфични за всяко звено от общинската администрация или с общо предназначение.

Чл. 2. Потребителите на информационни системи в администрацията на Община Сопот са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3. Секретарят на Община Сопот е административният ръководител по осъществяване на концепцията за е-община, като той може да делегира функции и на друг служител от администрацията, определен с изрично негово възлагане.

Чл. 4. При необходимост, по предложение на ръководителите на звена в общинската администрация, се определя служител от всяко звено, който оказва съдействие при подготовката на данни за въвеждане, разяснява и конкретизира специфичната дейност, подлежаща на автоматизиране.

Чл. 5. Създаването, разместването, преконфигурирането на работни места в администрацията на Общината, на чието разположение са или се предвижда да бъдат предоставени компютри се съгласува с Системния администратор и със Секретаря на Общината.

Глава втора
ПЛАНИРАНЕ, ПРОЕКТИРАНЕ И ИЗГРАЖДАНЕ НА ИНФОРМАЦИОННИ СИСТЕМИ

Чл. 6. Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Българската национална

рамка за оперативна съвместимост на информационните системи в изпълнителната власт (приета с Решение N 482 на МС от 28 юни 2006 г.), Наредба за общите изисквания за мрежова и информационна сигурност (Приета с ПМС № 279 от 17.11.2008 г., загл. изм. - ДВ, бр. 5 от 2017 г., в сила от 01.03.2017 г.) и Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги (Приета с ПМС № 3 от 09.01.2017 г., в сила от 01.03.2017 г.).

Чл. 7. Проектирането и изграждането на информационни и комуникационни системи, свързани с работата на звената от общинската администрация, включително и при необходимост от взаимодействие с информационни системи извън рамките на администрацията се извършва от или с участие на Системния администратор, съгласувано със Секретаря на Общината.

Глава трета
БАЗИ ДАННИ

Чл. 8. Форматите на електронните бази данни се определят съобразно нормативните актове и стандарти в тази област.

Чл. 9. При наличие на изисквания към съдържанието и структурата на бази данни, поставени с нормативни документи, създаваните и използвани бази данни задължително се съобразяват с тези изисквания.

Чл. 10. Всички действия по подготовката на данни за въвеждане в информационна система, а именно: събиране, актуализиране, сортиране и подреждане се извършват съобразно организация, създадена в съответните звена.

Чл. 11. Въвеждането и актуализацията на така подготвените данни с цел създаване на електронни бази данни се извършва от съответните служители по звена, съобразно длъжностните им характеристики и при спазване на определените права на достъп.

Чл. 12. Служителите на съответните работни места, които въвеждат и актуализират електронни бази данни са длъжни да ги поддържат в актуално състояние.

Чл. 13. Всички оригинали, които съдържат данни, предвидени за въвеждане, обработка с компютър, съхраняване или публикуване се подписват от съответния служител, подготвил данните, като с това се гарантира верността на подаваната за обработка информация.

Чл. 14. Служителите, извършващи въвеждане и актуализация на данните носят отговорност за тяхната достоверност.

Чл. 15. Издаването на документи при използване на съответната електронна база данни се извършва от служителите по звена съобразно длъжностните им характеристики и вменените им със заповед на Кмета на Общината задължения.

Чл. 16. При ползване на обща база от данни за извършване на административни услуги и наличие на достъп до нея, служителите са задължени да издадат искания документ независимо от мястото на поискването му.

Чл. 17. Обменът и предоставянето на електронни бази данни, собственост на Община Сопот по смисъла на Закона за авторското право и сродните му права с други институции, организации и фирми става само след одобряване от Кмета на Общината и съгласно приетите с Наредба за определянето и администрирането на местните такси и цени на услуги на Община Сопот цени за съответния вид данни.

Чл. 18. Системния администратор създава на сървър места за съхраняване на данни за всяко едно от звената, където служителите правят копия на файловете, с които работят, както и архивиране на данните, разположени на сървърите.

Чл. 19. За общо ползване от всички служители са предвидени:

1. деловодна система с права за достъп съобразно длъжностите и длъжностните характеристики на служителите;

2. вътрешен информационен портал.

Чл. 20. Правата за достъп до бази данни се определят съобразно длъжностните характеристики на служителите и вменените им със заповеди на Кмета на Общината задължения.

Чл. 21. Правата на достъп до общи бази данни за определено звено са както следва:

1. въвеждане и корекция на данните - по гореизложения ред, като идентифицирането на съответния служител става с дадените му потребителско име и парола за работа в локалната мрежа;

2. разглеждане на данните - в зависимост от предмета на дейност на съответното звено и необходимата за дейността му информация, които се определят съобразно потока на информацията в администрацията на Общината, мястото на съответно звено във функционалната структура на администрацията на Общината, длъжностните характеристики на съответните служители и заповеди на Кмета на Общината.

Чл. 22. На служителите на администрацията на Община Сопот, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици) се забранява:

1. да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга);

2. да ги използват извън рамките на служебните си задължения;

3. да ги предоставят на външни лица без да е заявена услуга.

Чл. 23. За нарушение целостта на данните се считат следните действия:

1. унищожаване на бази данни или части от тях;

2. повреждане на бази данни или части от тях;

3. вписване на невярна информация в бази данни или части от тях.

Чл. 24. Системния администратор предлага и реализира концепции за защита и опазване на електронните бази данни.

Чл. 25. Събирането, подготовката и въвеждането на данни директно в специфични раздели на интернет страницата се извършва от служители на администрацията на Община Сопот, определени от ръководителите на звената. На посочените длъжности лица се създават потребителски имена и пароли за извършване на актуализациите.

Чл. 26. За всички останали раздели на интернет страницата Секретарят на Общината и Зам.-кмета разпореждат събирането и подготовката на данните от служители в техния ресор, след което данните се пращат в електронен вид (на файлове) на e-mail sekretar_sopot@.abv.bg от където се поставят на интернет страницата на Общината от или се предоставят за поставяне на фирмата, която поддържа страницата.

Чл. 27. Данните, предвидени за публикуване на чужди езици се превеждат по установения в администрацията на Общината ред и се въвеждат на страницата по установения в тези Правила ред.

Чл. 28. Данните, предвидени за публикуване в интернет страницата на Община Сопот се обработват съобразно установения в тези Правила ред.

Глава четвърта
ПРОГРАМНИ ПРОДУКТИ

Чл. 29. Системните програмни продукти се избират от специалисти при съобразяване с политиката на държавната администрация в тази област.

Чл. 30. Функциите на приложните програми се създават съобразно изискванията на специалистите от съответните звена, които ще работят с тях и в съответствие с предмета на дейност на звеното, определен от длъжностните характеристики на неговите служители.

Чл. 31. Създаването на програмни продукти се възлага съобразно действащите нормативни документи, свързани с електронното управление и по реда на ЗОП, задължително съгласувано със специалисти.

Чл. 32. Разработката, надграждането или доставката на приложни програмни продукти за нуждите на съответните звена от администрацията става само при наличие на писмено задание за функциите на приложните програми, утвърдено от ръководителите на звената.

Чл. 33. Програмните менюта се създават с максимално възможно удобство за потребителя и при спазване на основните изисквания, посочени в Наредба № 7 от 15.08.2005 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи (Изд. от Министъра на труда и социалната политика и министъра на здравеопазването, обн., ДВ, бр. 70 от 26.08.2005 г.).

Чл. 34. Идентифициране и отстраняване на проблеми в работата, както и инсталация на програмни продукти, разработени от трети лица се извършва на място под контрола на Системния администратор. За извършване на тези дейности може да бъде осигурен и канал за връзка, който се изгражда от Системния администратор по начин и със средства, така че да не се допусне неконтролиран достъп до компютърната мрежа на общинската администрация на външни лица.

Глава пета
ТЕХНИЧЕСКО ОСИГУРЯВАНЕ - КОМПЮТЪРНА И ПЕРИФЕРНА ТЕХНИКА

Чл. 35. Техническото осигуряване се избира с оглед на изискванията на програмните продукти, които ще се използват на съответното работно място, както и със състоянието и тенденциите за развитие на компютърните технологии. Необходимото оборудване, независимо от източника и начина на придобиването му, се определя от Системния адмистратор, съгласувано с Гл. счетоводител по разпореждане на Кмета на Общината.

Чл. 36. Подмяна на части, добавяне на компоненти, принадлежности и други за подобряване на компютърните конфигурации, както и текуща подмяна на дефектирала техника се извършват по преценка на Системния администратор и по разпореждане на Секретаря на общината, съгласувано с Гл. счетоводител.

Чл. 37. Инсталирането на компютърните конфигурации, системните и приложните програми, както и следващи промени в тях се прави само от Системния администратор или упълномощените за това фирми - доставчици на компютърна, периферна техника и програмни продукти, но задължително в присъствие на служителя.

Чл. 38. Гаранционното обслужване на техниката се извършва само от упълномощените за това фирмени сервизи.

Чл. 39. Техническото обслужване (поддръжка), доколкото това не изисква намеса на упълномощен сервиз и дейности по ремонт, се извършва от Системния администратор. Извънгаранционно абонаментно и сервизно обслужване се извършва след избор на изпълнител по реда на ЗОП.

Чл. 40. Компютърна и периферна техника, която не се използва, се предава на Секретаря на Общината, като по негова преценка техниката се пренасочва към работни места, които имат нужда от такава или се предава на домакина за съхранение.

Чл. 41. Внасянето и изнасянето на компютърна и периферна техника от административните сгради на Община Сопот става само със знанието на Секретаря на Общината, в присъствието на домакина и с попълнена разписка по образец или при наличие на съответния предавателно-приемателен протокол.

Глава шеста
ИЗПЪЛНЕНИЕ НА ПРОГРАМИ И ПРОЕКТИ

Чл. 42. Създаването и доставката на софтуерни приложения, интернет страници и други решения, свързани с развитието на информационните технологии, включително доставката на хардуер и софтуерни лицензи, които се извършват чрез външно финансиране по проекти на общинската администрация, се съгласуват със Системния администратор, както следва:

1. на етап проектно предложение;
2. на етап техническо задание за провеждане на обществена поръчка.

Чл. 43. При необходимост Системния администратор оказва методическа помощ при изпълнение на одобрените проекти, съдържащи решения в сферата на информационните технологии.

Глава седма
РАБОТНО МЯСТО

Чл. 44. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 45. Работното място се оборудва при спазване на изискванията на Наредба № 7 от 15.08.2005 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи (Изд. от Министъра на труда и социалната политика и Министъра на здравеопазването, обн., ДВ, бр. 70 от 26.08.2005 г.).

Чл. 46. Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения съобразно изискванията на Приложение № 11 към чл. 45 ал. 2 от Наредба за общите изисквания за мрежова и информационна сигурност (Приета с ПМС № 279 от 17.11.2008 г., загл. изм. ДВ бр. 5 от 2017 г.).

Чл. 47. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място или ползвани от него на сървъра на локалната компютърна мрежа, съобразно дадените му права.

Чл. 48. Забранява се на външни лица работата с персоналните компютри на администрацията на Община Сопот, освен за упълномощени фирмени специалисти в случаите на първоначална инсталация на компютърна и периферна техника програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствие на служителя.

Чл. 49. Забранява се използването на преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на администрацията на Община Сопот, за неслужебни цели.

Чл. 50. Преди работа с информационни носители с възможност за презаписване на данни, специалистите на съответното работно място ги проверяват за наличие на компютърни вируси.

Чл. 51. Служители, които съхраняват електронни данни на компютъра, който ползват, са длъжни периодично да правят и съхраняват копие от тези данни върху външен носител, като съхраняват тези носители в подходящи кутии и/или шкафове, достъпни само за упълномощени служители, на места с температура не по-ниска от 10 градуса и по-висока от 50 градуса, относителна влажност не по-ниска от 20 и по-висока от 80 % и далеч от магнити или намагнитени предмети.

Чл. 52. Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни

мрежи, на комуникационни устройства се извършва само след съгласуване със Секретаря на Общината и само от Системния администратор.

Чл. 53. Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

Чл. 54. Всички комуникационни шкафове се заключват, като ключове от тях се намират при Секретаря на Общината.

Чл. 55. В помещение, където се съхраняват електронни бази данни и програмни продукти на магнитни и магнито-оптични носители, оставането на служители в извънработно време става само при възложена конкретна задача, за чието изпълнение оставането е наложително и при спазване на разпоредбите за достъп в сградата на администрацията на Община Сопот.

Глава осма
ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 56. Системния администратор извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща на администрацията на Община Сопот след получаване на заявка по образец. Заявката се предоставя в електронен вид на Секретаря на Община Сопот (на e-mailsekretar_sopot@abv.bg.) от ръководителя на звеното, в което работи служителят, за когото се отнася заявката. Секретарят я предава на Системния администратор.

Чл. 57. Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола.

Чл. 58. Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.

Чл. 59. Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронна поща при използване на предоставените им потребителски имена и пароли. Паролите трябва да се сменят на всеки шест месеца и трябва да съдържат най-малко осем символа. Символите трябва да бъдат с минимум една главна буква, малки букви, цифри и специален знак.

Чл. 60. Компютрите, свързани в мрежата на администрацията на Община Сопот използват интернет само от доставчик, с когото Община Сопот има сключен договор за доставка на интернет след провеждане на процедура по реда на ЗОП.

Чл. 61. Забранява се свързването на компютри едновременно в мрежата на администрацията на Община Сопот и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на Община Сопот и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и Наредба за общите изисквания за мрежова и информационна сигурност (Приета с ПМС № 279 от 17.11.2008 г., загл. изм. - ДВ, бр. 5 от 2017 г., в сила от 01.03.2017 г.).

Чл. 62. (1) Забранява се инсталирането и използването на комуникатори (като icq, skype, messenger, facebook и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на Община Сопот и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на администрацията на Община Сопот.

(2) Изключения по ал. 1 се допускат само с изрично разпореждане на Кмета на Община Сопот.

Чл. 63. Забранява се съхраняването на сървърите на администрацията на Община Сопот на лични файлове с текст, изображения, видео и аудио.

Чл. 64. Забранява се отварянето без контрол от страна на отговорни служители на:

1. получени по електронна поща или на преносими носители изпълними файлове, файлове с мобилен код и файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg и архивни файлове;
2. получени по електронна поща съобщения, които съдържат неразчитаеми знаци.

Глава девета
ПРАВА НА ДОСТЪП ДО ИНФОРМАЦИОННИ РЕСУРСИ

Чл. 65. При назначаване на нов служител или служител по заместване, мл. експерт „Човешки ресурси" уведомява за това Секретаря на Общината не по-късно от 3 работни дни преди датата на назначаване. След постъпване на работа новоназначеният служител представя при Секретаря на Общината попълнена заявка по образец или копие от заповед, издадена на основание чл. 44, ал. 1, т. 14 от ЗМСМА или чл. 24, ал.4 от Закона за защита на личните данни, на основание на която му се определят права на достъп до определени ресурси. Заявката може да се предостави и в електронен вид (на e-mail sekretar_sopot@abv.bg) на Секретаря на Общината от ръководителя на звеното, в което работи служителят, за когото се отнася заявката. Секретарят препраща заявката до Системен администратор за изпълнение.

Чл. 66. За промяна в правата на достъп служителят представя на Секретаря на Общината заявка по образец. Заявката може да се предостави и в електронен вид (на e-mail sekretar_sopot@abv.bg) на Секретаря на Общината от ръководителя на звеното, в което работи служителят, за когото се отнася заявката. В случай, че основанията за промяна са документи като заповеди, длъжностна характеристика и др., към заявката се изискват копия и/или се прави справка за съдържанието им.

Чл. 67. При прекратяване на служебното (трудовото) правоотношение между администрацията на Община Сопот и определен служител, мл. експерт „Човешки ресурси" уведомява за това Секретаря на Общината не по-късно от 3 работни дни преди датата на прекратяване. С изтичане на работния ден, предхождащ прекратяването на правоотношенията на служителя с Община Сопот, Системния администратор прекратява правата на достъп до мрежови ресурси, електронна поща и компютър на служител, чието служебно (трудово) правоотношение с Община Сопот се прекратява и при необходимост извършва преинсталация на компютъра.

Чл. 68. В случаите, когато се прекратява служебното (трудово) правоотношение на служител от администрацията, но същият работи по проект на Община Сопот, който не е приключил, потребителското му име може да бъде съхранено за срока на проекта, като за тази цел ръководителят на проекта информира по електронна поща Секретаря на Общината, като изрично посочи и срока на проекта.

Глава десета
ОЦЕНКА И УПРАВЛЕНИЕ НА РИСКА

Чл. 69. Рискът за сигурността е фактическо състояние, което създава заплахи за уязвяване на един или няколко информационни актива, което да предизвика тяхното повреждане или унищожаване.

Чл. 70. Оценката на риска се дефинира чрез определяне на вероятността за уязвяване въз основа на ефективността на съществуващите или планираните мерки за сигурност.

Чл. 71. Заплахите за мрежовата и информационна сигурност се класифицират по следните критерии:

1. по елементите на информационната сигурност (достъпност, цялостност, конфиденциалност), към които са насочени;

2. по компонентите на информационната система (апаратура, софтуер, данни, поддържаща инфраструктура), към които са насочени;

3. по начина на осъществяване (случайни/преднамерени действия, от природен/технологичен характер и др.);

4. по разположението на източника (вътре във/извън информационната система).

Чл. 72. Действията по управление на риска обхващат оценка на неговия размер, изработване на ефективни и икономични мерки за неговото снижаване и оценка дали резултативния риск е в приемливи граници. Управлението на риска се извършва чрез последователно прилагане на два типа циклично повтарящи се действия:

1. оценка (преоценка) на риска

2. избор на ефективни и икономични средства за неговата неутрализация.

Чл. 73. При идентифициране на риск се предприема едно от следните действия:

1. ликвидиране на риск (например чрез отстраняване на причиняващите го обстоятелства);

2. намаляване на риска (например чрез използване на допълнителни защитни средства);

3. приемане на риска и разработване на план за действие в обстановка на риск;

4. преадресиране на риска (например чрез сключване на съответната застраховка).

Чл. 74. Процесът на управление на риска включва следните етапи:

1. избор на анализируемите обекти и нивото на детайлизация на анализа;

2. избор на методология за оценка на риска;

3. идентификация на информационните активи;

4. анализ на заплахите и последствията от тях, откриване на уязвимите места в защитата;

5. оценка на рисковете;

6. избор на защитни мерки;

7. реализация и проверка на избраните мерки;

8. оценка на остатъчния риск - явява се начало на нов цикъл на оценка, който се провежда ако остатъчният риск не удовлетворява ръководството на администрацията. Оценка на остатъчния риск се извършва минимум веднъж в годината.

Чл.75. Видовете заплахи срещу мрежовата и информационната сигурност, формулирани в международния стандарт ISO/IEC TR 13335:2000, които могат да застрашат конфиденциалността, интегритета и достъпността, са следните:

1. Подслушване, изразяващо се в достъп до служебна информация чрез прихващане на електронни съобщения, независимо от използваната технология.

2. Електромагнитно излъчване, изразяващо се в действия на трето лице, целящо да получи знание за обменяни данни посредством информационна система.

3. Нежелан код, който може да доведе до загуба на конфиденциалността чрез записването и разкриването на пароли и до нарушаване на интегритета при интервенции от трети лица, осъществили нерегламентиран достъп с помощта на такъв код. Нежелан код може да се използва, за да се заобиколи проверка за достоверност, както и всички защитни функции, свързани с нея. В резултат кодът може да доведе до загуба на достъпността, когато данните или файловете са разрушени от лицето, получило нерегламентиран достъп с помощта на нежелан код.

4. Маскиране на потребителската етичност може да доведе до заобикаляне на проверката за достоверност и всички услуги и защитни функции, свързани с нея.

5. Погрешно насочване или пренасочване на съобщенията може да доведе до загуба на конфиденциалност ако се осъществи нерегламентиран достъп от трети лица. Погрешното насочване или пренасочване на съобщенията може да доведе и до нарушаване на интегритета, ако погрешно насочените съобщения са променени и след това насочени към първоначалния адресат. Погрешното насочване на съобщения води до загуба на достъпността до тези съобщения.

6. Софтуерни грешки могат да застрашат конфиденциалността ако софтуерът е създаден с контрол на достъпа или за криптиране или ако грешката в софтуера осигури възможност за нежелан достъп в информационната система.

7. Кражбата на информационни активи може да доведе до разкриване на информация, която представлява служебна или друга защитена от закона тайна. Кражбата може да застраши достъпността до данните или информационното оборудване.

8. Нерегламентиран достъп до компютри, информационни ресурси, услуги и приложения може да доведе до разкриване на поверителни данни и до нарушаване интегритета на тези данни, ако нерегламентираната им промяна е възможна. Нерегламентираният достъп до компютри, данни, услуги и приложения може да наруши достъпността до данните, ако тяхното изтриване или заличаване е възможно.

9. Нерегламентиран достъп до носител на данни може да застраши съхраняваните върху него данни.

10. Повреждане на носител на информация може да наруши интегритета и достъпността на данните, които се съхраняват на този носител.

11. Неизвършването на редовна поддръжка на информационните системи или допускане на грешки по време на процеса по поддръжка може да доведе до нарушаване на достъпността до данни.

12. Аварии в електрозахранване и климатични инсталации могат да доведат до нарушаване на интегритета и достъпността до данни, ако вследствие на настъпването на авариите са увредени информационни системи или носители на данни.

13. Технически аварии (например аварии в мрежите) могат да нарушат интегритета и достъпността до информация, която се съхранява или разпространява чрез тази мрежа.

14. Грешки при предаването на информацията могат да доведат до нарушаване на нейната цялост и достъпност.

15. Употреба на нерегламентирани програми и информация могат да нарушат интегритета и достъпността до данните, съхранявани и разпространявани чрез информационна система, в която е настъпило такова събитие, и програмите и информацията се използват, за да се изменят и съществуващи програми и данни по неразрешен начин или ако те съдържат нежелан код.

16. Потребителски грешка могат да нарушат интегритета и достъпността до данни чрез неумишлено или умишлено действие.

17. Липса на потвърждаване може да застраши интегритета на данните. Предпазните мерки за предотвратяване на непотвърждаването трябва да се прилагат в случаите, когато е възможно да се получи доказателство за това, че дадено съобщение е изпратено и е/не е получено, както и за това, че мрежата е пренесла съобщението.

18. Интервенции срещу интегритета на данните могат да доведат до тяхното сериозно увреждане и до невъзможност от по-нататъшното им използване.

19. Аварии в комуникационното оборудване и услуги могат да увредят достъпността на данните, предавани чрез тези услуги.

20. Външни въздействия с огън, вода, химикали и други могат да доведат до увреждане или унищожаване на информационното оборудване.

21. Злоупотреба с ресурси може да доведе до недостъпност до данни или услуги.

22. Природни бедствия могат да доведат до унищожаване на данни и информационни системи.

23. Предотвратяване на комуникационния трафик може да доведе до нарушаване на достъпността до обменяни данни.

Чл. 76. Идентифицирането, оценката и управлението на рисковете за мрежовата и информационна сигурност се извършва в сроковете, по методиката и във формата, приети в Правилата за управление на риска н Община Сопот, както следва:

1. Системния администратор анализира и оценяват рисковете, свързани с общото състояние на инфраструктурата и прилагането на информационни и комуникационни технологии (ИКТ) в Община Сопот. Рисковете с високо и средно влияние и вероятност се докладват на Секретаря на Община Сопот с предложение за възможните за предприемане мерки.

2. Дирекциите - собственици на значими информационни системи, анализират и оценяват специфични за системите рискове, с ниво на детайлизация, позволяващо реална оценка на рисковете и избор на конкретни защитни мерки. Идентифицирането, анализът и оценката на тези рискове се извършва съвместно от дирекцията/ите - собственици.

Чл. 77. Чрез оценката на риска относно мрежовата и информационна сигурност се идентифицират неприемливи опасности, за които се налага да се предприемат действия. За опасностите, които са на приемливо ниво, е необходимо да се предприемат мерки за контрол така, че да се държат в приемливи граници. След като идентифицираните рискове се оценят със Заповед на Кмета на Община Сопот се назначава работна група по управление на рисковете, която да взема решение относно подходящата реакция по чл. 73 към всеки от рисковете, като съобразяват решението си с риск апетита на Община Сопот.

На база на избраната реакция на рисковете се определят съответните контролни цели и конкретни контролни дейности, които се вписват в плана за действие. Броят и обхватът на контролните дейности трябва да е достатъчен, за да даде увереност, че съществените рискове за мрежовата и информационната сигурност са ограничени до приемливи нива в рамките на риск апетита на Общината.

Глава единадесета
КОНТРОЛ

Чл. 78. Ръководителите на звена от администрацията контролират използването на компютърната и периферна техника, като при необходимост изясняват причините за неизползване на техниката и програмите или използването им не по предназначение и уведомяват Заместник-кмета и Секретаря на Общината с цел прилагане на съответните административни действия.

Чл. 79. Системния администратор следи за изпълнението на дейности, които засягат работата с електронни бази данни, ползване на сървърно дисково пространство, достъп до отдалечени ресурси, като при установяване на неизпълнение или лошо изпълнение по някоя от точките, касаещи работата с електронни данни предприемат действия за възстановяване на изправността и уведомява Секретаря на Общината с цел прилагане на съответните административни действия.

Чл. 80. На периодична проверка от Системния администратор подлежат веднъж годишно:

1. компютрите относно: промени в хардуерната конфигурация, инсталирания софтуер, допълнително инсталиран софтуер, неразрешени промени в BIOS или операционната система на компютъра;

2. сървърите относно: лични файлове с текст, изображения, видео и аудио.

Глава дванадесета
ДИСЦИПЛИНАРНА ОТГОВОРНОСТ

Чл. 81. В случаите, когато служителите са изискали закупуване на компютър, периферна техника и програмни продукти, но не ги използват или ги използват не по предназначение, Кметът по доклад от Секретаря на Общината изисква от служителите на ресорните им звена писмени обяснения за причините. При установяване на вината на служителите, последните се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 1, т. 9 от Кодекса на труда (КТ) или чл. 89, ал. 2, т.1 от Закона за държавния служител (ЗДСл).

Чл. 82. Служители, които не поддържат актуални данните, с които работят, въведат умишлено неверни данни и създават условия за разпространяване на невярна електронна информация, се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 1, точки 3, 4, 7, 8 и 10 от КТ или чл. 89, ал. 2 от ЗДСл и се задължават да възстановят данните в актуално състояние.

Чл. 83. Служители на администрацията на Община Сопот, които заразят програми и бази данни с компютърни вируси се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 1, т. 9 от КТ или чл. 89, ал. 2 от ЗДСл и със заплащане на стойността на повредените програми и на разходите за възстановяване на данните.

Чл. 84. Служители на администрацията на Община Сопот, извън Системния администратор, които деинсталират, инсталират или разместват компютърни конфигурации, части от тях, периферна техника, активни и пасивни компоненти на локални компютърни мрежи както и комуникационни устройства се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 1, т. 3 и т. 9 от КТ или чл. 89, ал. 2 от ЗДСл, а при повреда на техниката - и със заплащане на стойността на повредената техника.

Чл. 85. При установяване, че външни лица използват компютърна и периферна техника в администрацията на Община Сопот извън регламентираните в настоящите правила случаи, служителите на администрацията на Община Сопот допуснали това се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 1, точки 3, 8 и 9 от КТ или чл. 89, ал. 2 от ЗДСл, а при установяване на повреди на техника, данни и програми и със заплащане на стойността на повредените техника и програми, както и на разходите за възстановяване на данните.

Чл. 86. При установяване на действия на служителите съгласно чл. 22 и чл. 23 от настоящите правила или при установяване, че служителите са унищожили служебна информация, разположена на ползваните от тях компютри, служителите се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 1, точки 3, 8 и 9 от КТ или чл. 89, ал. 2 от ЗДСл.

Чл. 87. Служители на администрацията на Община Сопот, които в установеното работно време не изпълняват служебните си задължения и поставените им задачи, а използват компютрите за компютърни игри или за друг вид дейност, която не е свързана с изпълнението на служебните им задължения, се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 1, т. 1 и т. 3 от КТ или чл. 89, ал. 2 от ЗДСл.

Чл. 88. При следващи нарушения на провинилия се служител се налагат следващите по степен дисциплинарни наказания съгласно чл. 188 от КТ или чл. 90 от ЗДСл.

Глава тринадесета
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1, Ръководителите и служителите в Общинска администрация гр. Сопот са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. В допълнение към тези правила се разработват конкретните политики и процедури в съответствие с изискванията на международния стандарт за информационна сигурност ISO 27001 съобразно Наредба за общите изисквания за мрежова и информационна сигурност.

§ 3. Контролът по спазване на правилата се осъществява от Кмета на Общината, Заместник-Кмета на Общината, Секретаря на Общината и Директорите на дирекции.

§ 4. Настоящите Правила влизат в сила от 16.12.2019 г.