

УТВЪРЖДАВАМ:

МАРИН РАЧЕВ

КМЕТ

Заличено на основание чл. 5,
параграф 1, буква „в” от Регламент
/ЕС/ 2016/679

СМВРИ

КМЕТ

ЕМВРИ

ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

Изготвил:

Пенка Райков

експерт ИОТ

Съгласувал:

Виолета Близна

ист

Заличено на основание чл. 5,
параграф 1, буква „в” от Регламент
/ЕС/ 2016/679

РАЗДЕЛ I

ВЪВЕДЕНИЕ

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

РАЗДЕЛ II

ЦЕЛИ

2. Целите на настоящата политика са:
 - осигуряване на непрекъснатост на работните процеси;
 - минимизиране на рисковете за сигурността на информацията, причиняващи загуби или вреди на Община Септември;
 - минимизиране на степента на загуби или вреди, причинени от пробиви в информационната сигурност;
 - осигуряване на необходимите ресурси за поддържане на ефективно управление на информационната сигурност;
 - информиране на служителите за техните отговорности и задължения по отношение на информационната сигурност;
 - осигуряване на съответствие с нормативни изисквания.
3. Ръководството на Община Септември ще прилага следните основни принципи при управление на информационната сигурност:
 - 3.1. От законова гледна точка:
 - защита на данни и неприкосновеност на лична информация;
 - опазване на архивите на институцията;
 - защита на авторски права, търговска информация и други права върху интелектуална собственост.
 - 3.2. От общоприетите добри практики за информационна сигурност:

- разработване на политика по информационна сигурност;
 - разпределяне на отговорностите по информационна сигурност;
 - обучение по информационна сигурност;
 - докладване на инциденти, свързани със сигурността;
 - управление непрекъснатостта на работа;
 - дисциплинарен процес в следствие от нарушенията на политиката по сигурност.
4. Стратегическа цел на Община Септември за въвеждане на тази политика е, че тя дефинира мястото ѝ по отношение на мисията и целите на Община Септември и установява общи правила за поведение.

РАЗДЕЛ III

ОБХВАТ НА СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

5. Системата за управление на информационната сигурност обхваща всички документи - електронни и на хартиен носител, както и:
- бази данни;
 - компютри – настолни и преносими;
 - софтуерни активи;
 - локална мрежа и мрежи в изнесените работни места;
 - всички WEB базирани и други информационни системи на Община Септември;
 - носители на информация (дискове, USB памети и др.);
 - устройства за копиране и предаване на данни;
 - комуникационни устройства;
 - инфраструктура на Община Септември (електрозахранване, кабели за локална мрежа и др.);
 - служители.
6. Системата за управление на информационната сигурност обхваща всички структурни звена и кметства.
7. Тази политика не се отнася за документи и процеси свързани с класифицирана информация и попадащи под обхвата на ЗЗКИ.

РАЗДЕЛ IV

ПРИОРИТЕТИ

8. Ръководството на Община Септември насочва внимание и полага усилия:
- критичната (чувствителната) информация и системи да бъдат подлагани на редовен анализ по отношение на риска;
 - за критичните (чувствителни) информационни ресурси и системи да бъдат определени

- служители, отговорни за конкретните работни приложения, компютри и мрежи;
- информацията да бъде класифицирана по начин, който показва нейната критичност и чувствителност;
 - служителите да бъдат информирани и да осъзнават проблемите на информационната сигурност;
 - да бъде създадена организация на работа, която гарантира спазване на авторски права на компютърния софтуер, както и условията за работа с тях;
 - нарушаването на политиката по сигурността и евентуалните недостатъци в системата за информационна сигурност да бъдат докладвани;
 - информационните ресурси да бъдат защитавани от гледна точка на изискванията за конфиденциалност, цялостност и достъпност.
9. Въвеждането и спазването на политиката по информационна сигурност цели да се забранят:
- използването на информацията и системите на организацията без оторизация или за цели, които не са свързани с дейността ѝ;
 - изнасяне на оборудване или информация без оторизация;
 - неоторизирано копиране на информация и софтуер;
 - компрометиране на пароли (например със записване или разпространяване);
 - използване на персонална информация за други цели, освен ако няма изрична оторизация;
 - фалшифициране на доказателства в случай на инцидент;
 - отправяне на неприлични, дискриминационни или нападателни изявления, които могат да бъдат противозаконни (например с използване на електронна поща или интернет);
 - разпространение на незаконни материали (например с неприлично или дискриминационно съдържание).

РАЗДЕЛ V

РОЛИ И ОТГОВОРНОСТИ

10. За осъществяване на настоящата политика и за осигуряване на информационната сигурност, се определят следните отговорности:

10.1. Ръководството на Община Септември:

- формулира, преглежда и изменя Политиката по информационна сигурност при необходимост;
- оценява потребностите и осигурява необходимите ресурси за прилагане на пропорционални и адекватни на рисковете организационни, технически и технологични мерки, гарантиращи високо ниво на мрежова и информационна сигурност;
- разпределя ролите и отговорностите, свързани със сигурността на информацията;

- координира прилагането на мерки за защита и информационна сигурност.

10.2. Служител, отговарящ за мрежовата и информационна сигурност:

- изпълнява възложени дейности, свързани с прилагане на Политиката и мерките по осигуряване на информационна сигурност;
- отговаря за изготвяне на оценка на риска и за класификация на информацията;
- извършва оценка на риска и адекватност на мерките при изменения в информационната система;
- при възникнала необходимост предлага нови, спешни и ефикасни мерки за подобряване на сигурността;
- съдейства за осигуряване на обучението и осъзнаването на потребителите на информационната система.

10.3. Системни администратори, които:

- отговарят за управление и поддържане на интернет, електронна поща, сървъри, локална мрежа, архивиране, техническа защита (софтуер и хардуер) от вреден софтуер;
- нива на достъп;
- проследимост на включване и опити за включване;
- изготвяне и поддръжка на цялостната документация, свързана с администрирането на информационната система и нейните подсистеми.

10.4. Потребители:

- потребителите на информационните и комуникационни ресурси, се задължават да следват процедурите, инструкциите и заповедите, свързани с информационната сигурност, да докладват за проблеми и инциденти в информационната система;
- носят отговорност за правилното опазване и използване на поверените им ресурси.

РАЗДЕЛ VI

ОЦЕНКА НА РИСКА

11. Оценката на риска се прилага за всеки актив на Община Септември или извън нея, обхванат от споразумение с трета страна. Оценката на риска се прилага към цялата информационна система и включва приложения, сървъри, мрежа, всеки процес или процедура, чрез които системата се администрира и/или поддържа.
12. Идентифицирането и оценката на риска се извършва на базата на разработени и утвърдени в Община Септември Вътрешни правила за анализ и оценка на риска.
13. Служителят, отговарящ за мрежовата и информационна сигурност извършва идентифициране, оценка и управление на рисковете, свързани с информационната сигурност на Община Септември, като документира процеса в утвърдената форма – риск-регистър.

14. Резултатите от оценката на риска определят мерките за контрол за намаляване на риска в съответствие с нивата на риска.
15. Оценката на риска се извършва периодично, за да бъдат отчетени измененията в изискванията за сигурност, активите, заплахите, уязвимостите, въздействията или други настъпили промени.

РАЗДЕЛ VII

ВЪТРЕШНА ОРГАНИЗАЦИЯ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

16. Ръководството на Община Септември провежда политика за координиране на цялата дейност в организацията по внедряването и поддържането на мерките за защита.
17. Разпределяне на отговорностите по сигурността на информацията се извършва в съответствие с приета от Община Септември Политиката информационна сигурност.
18. Отговорностите на служителите се определят в съответствие с настоящата политика, в правила, заповеди или в длъжностните им характеристики.
19. Служителят, отговарящ за мрежовата и информационна сигурност предлага на ръководството за одобрение разпределението и документирането на отговорностите за изпълнението на следните дейности:

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

РАЗДЕЛ VIII

УПРАВЛЕНИЕ НА АКТИВИТЕ

20. Политиката се отнася до служители, договарящи страни, консултанти, временно работещи за Община Септември (стажанти) и други, включително и служители на трети страни. Тази политика се отнася до цялото информационно и комуникационно оборудване, собственост или използвано от Община Септември, включително кметствата.
21. Политиката на Община Септември за използване на активите цели не да налага ограничения, противоречащи на установената култура на откритост и доверие, а да

- защитава служителите на Община Септември и самата нея от незаконни и увреждащи действия, извършени предумишлено или несъзнателно.
22. Системите, свързани с интернет, локална мрежа, включително компютърното оборудване, приложния софтуер, операционните системи, средствата за съхранение на информация, електронната поща и други са собственост на Община Септември. Тези системи са предназначени да се използват за целите на дейността и в интерес на организацията.
 23. Данните, които потребителите обработват и съхраняват при изпълнение на служебните си задължения са собственост на Община Септември.
 24. За всяка друга информация, съхранявана на технически средства на Община Септември не се гарантира конфиденциалност. Служителите са задължени да правят добра преценка относно разумността на съхраняване на информация върху служебни технически средства за лична употреба.
 25. За целите на сигурността и поддръжката на мрежата, системните администратори наблюдават оборудването, системите и мрежовия трафик по всяко време.
 26. Община Септември си запазва правото чрез системните администратори да деинсталира всякакъв софтуер или файлове, които не са свързани със служебните задължения на потребителя. Примери за такъв софтуер или файлове включват, но не се ограничават до: игри, музикални файлове, файлове с изображения, споделени и безплатни програми, и др.
 27. Община Септември си запазва правото периодично да одитира мрежите и системите, за да провери спазването на тази политика.
 28. Служителите трябва да прилагат изключително внимание когато работят с електронната поща, за да се предпазят от вируси, троянски коне и друг вредоносен софтуер.

РАЗДЕЛ ІХ

СИГУРНОСТ, СВЪРЗАНА С ЧОВЕШКИТЕ РЕСУРСИ

29. Сигурността на човешките ресурси на Община Септември е насочена основно към осъзнаване на необходимостта от осигуряване на информационната сигурност чрез адекватно дефиниране на отговорности и обучение.
30. Администрирането на човешките ресурси обхваща целия процес - от проучване на кандидатите, назначаване, определяне на задълженията, промяна на длъжността и до прекратяване на договорите включително.
31. Всички служители на Община Септември се задължават да спазват утвърдените правила и процедури, свързани с мрежовата и информационна сигурност, определени в политиката и вътрешните актове на общината. Това обстоятелство се удостоверява чрез декларация, която служителите подписват при постъпване на работа.
32. В договорите с лица, по силата на които последните обработват информация на Община Септември, задължително се включват клаузи за спазване на конфиденциалност и/или физическите лица, които фактически изпълняват дейностите, подписват декларации за конфиденциалност, съгласно **Приложение № 1**.
33. В случаи на сериозно нарушение на политиката и правилата за сигурност на човешките ресурси се прилага дисциплинарен процес, който включва отнемане на права за достъп до информационни ресурси, на активи и ако е необходимо, отстраняване от работа.

РАЗДЕЛ X

ФИЗИЧЕСКА СИГУРНОСТ, СИГУРНОСТ НА ЗАОБИКАЛЯЩАТА СРЕДА И КОНТРОЛ НА ДОСТЪПА

34. Информационните системи, които поддържат критични за Община Септември дейности, притежават подходяща физическа сигурност. Никакви конфиденциални материали в електронен формат не се оставят в неконтролирана среда и са защитени срещу случаен достъп.
35. Оборудването, което поддържа критични функции, се защитава физически от заплахи за сигурността и влияние на рискове от околната среда за предотвратяване на загуби, щети или излагане на риск на активи и прекратяване на основни дейности. Това включва информационно, комуникационно, мрежово оборудване, оборудване за съхранение на данни, хранващо оборудване и оборудване за контрол на околната среда.
36. Защитата на физическата сигурност се базира на подходящ контрол на достъп (ключове за ограничен достъп, входни точки за служителите, секретни ключалки, видеонаблюдение).
37. Изнасянето извън сградите на Община Септември и кметствата на информационните активи (собственост на общината или съответното кметство) изисква разрешение от съответния ръководител и подлежи на проверка.
38. Служебна информация не се оставя без надзор или контрол, което означава видима на екран.
39. Когато използването на дадено оборудване се прекрати, всички ключове, идентификационни карти и други устройства и пароли за достъп се връщат и отчитат.
40. При всички положения, когато информационната инфраструктура и/или физическата среда за разполагане, използвана от Община Септември е споделена или не е под пряк контрол, се гарантира с договорни условия, че настоящата политиката за информационна сигурност ще се спазва. Спазването на тези условия се проверява на място периодично и се включва в извършваните одити по сигурността.
41. Физическият достъп до ИТ съоръженията и комуникационното оборудване на Община Септември се извършва от и/или в присъствие на служители на Община Септември.
42. Средствата за контрол на физическата сигурност се използват и при защита на копирни машини, факсове и мрежови принтери.
43. Всички информационни системи на Община Септември работят във физически условия, дефинирани от техните производители.
44. Сървърното помещение на Община Септември е климатизирано. Осигурен е пожарогасител. Сървърното помещение е оборудвано с непрекъсваеми хранващи устройства.
45. Община Септември се стреми да създава, поддържа и осигурява условия за безопасна работа в съответствие със Закона за здравословни и безопасни условия на труда.
46. Политиката на Община Септември за контрол на достъпа е базирана на принципите „необходимост да знае“ или „необходимост да се ограничи“, „всеки достъп, който не е изрично разрешен е забранен“ и минимизиране на привилегиите.
47. Ръководството на Община Септември прилага мерки на контрол на достъп, които да осигурят:
 - физическа защита на информационните ресурси;

- достъп до съответните информационни ресурси в съответствие с политиката на собственика на ресурса и на ръководството на общината;
- определяне на нивата на достъп в съответствие с ролята, която трябва да изпълняват служителите на общината и нивата на класификация на информацията;
- механизми за контрол на физическо влизане;
- определяне на зони за обществен достъп, доставки и зареждане;
- контрол на нивото на достъп за всеки служител;
- разделяне на ролята за контрол на достъпа;
- минимизиране на необходимостта от специални привилегии;
- спазване на правилата за „чисто бюро и чист екран“;
- ограничаване нивата на достъп на външни потребители на информационните системи;
- отнемане на права на достъп при напускане;
- периодичен преглед на достъпа;
- ъпгрейд на контрола на достъп в отговор на нови заплахи, възможности, изисквания или изводи от инциденти.

РАЗДЕЛ XI

РАЗРАБОТВАНЕ, ВНЕДРЯВАНЕ И ПОДДЪРЖАНЕ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

48. Политиката на Община Септември по разработване, внедряване, изменение и поддържане на информационните системи е базирана на принципа на превантивната оценка на риска от измененията, включително ъпгрейд на съществуващи и внедряване на нови елементи от системата, разделение на средата за изпитване от действащата информационна система и планирана поддръжка на цялата информационна система.
49. С цел предотвратяване на грешки, загуба, неразрешено изменение или използване на информация в приложни информационни системи, се прилагат механизми за контрол върху входните данни, вътрешната обработка и изходните данни.
50. Разработването и внедряването на информационни системи се предхожда от анализ за необходимостта от тях, както и от ясно и конкретно дефиниране на процесите, които съответните системи предстои да обслужват.

РАЗДЕЛ XII

УПРАВЛЕНИЕ НА ИНЦИДЕНТИ И ПОДОБРЯВАНЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

51. В Община Септември следва да се събират данни и да се извършва анализ на вида и броя на инцидентите, на направените разходи по разрешаване на инцидентите. Целта е да се идентифицират повтарящите се инциденти или инцидентите с голямо влияние, да се ограничат честотата, щетите и загубите от появата им в бъдеще.
52. Всички потребители на информационните системи на Общината са задължени да докладват за наблюдавани събития и слабости в информационната сигурност.
53. Действията свързани с управление на инциденти включват докладване, анализ на причината, планиране на коригиращи и превантивни мерки за предотвратяване на повторна поява, възстановяване на системата и съобщаване на инцидента.
54. Действията за възстановяване след нарушение на сигурността и за коригиране на грешки на системите се извършва от системния администратор.

РАЗДЕЛ XIII

ОСИГУРЯВАНЕ НА НЕПРЕКЪСНАТОСТТА НА ДЕЙНОСТТА

55. Ръководството на Община Септември разбира необходимостта от планиране непрекъснатостта на дейността. Осъзнава, че има значителен риск за неговите критични процеси при потенциални и неочаквани разрушителни събития. Увеличаващото се развитие на процеси, базирани на технологии и силната зависимост от информационните технологии, е основание за създаване на план за непрекъснатост на работа.
56. Община Септември създава условия и следи за непрекъснатост на работата на критичните ресурси на системата при настъпване на сериозни неблагоприятни условия и опасност за прекъсване, по-голямо от 8 часа.

РАЗДЕЛ XIV

ПРИДОБИВАНЕ И ПОЛЗВАНЕ НА ЛИЦЕНЗИ

57. Община Септември създава организация на работа, която гарантира спазване на авторски права на компютърния софтуер, както и условията за работа с тях. Институцията предприема всички необходими действия за предотвратяване на копирането на лицензиран софтуер от потребителите, както и използването на свързана с него документация в изнесените работни места или на друго място, освен ако не съществува изрично разрешение за това, съгласно договора с лицензодателя.
58. Целият софтуер, придобит от Община Септември, трябва да бъде закупен след съгласуване със системния администратор.
59. За да се гарантира, че Община Септември поддържа пълна документация за закупения софтуер и може да регистрира, поддържа и актуализира съответния софтуер, каналите за придобиването му са ограничени.
60. Служителите използват софтуера по начин, който съответства на условията в договора, с който са предоставени лицензите.
61. Компютрите на Община Септември са активи, нейна собственост, използват лицензиран софтуер и са защитени от вируси.

62. Забранява се на потребителите да внасят софтуер отвън и да го инсталират на своите компютри. Притежаваният от Община Септември софтуер не може да бъде изнасян от потребителите и качван на други компютри.
63. Всички потребители използват наличния софтуер, при спазване на условията на съответните лицензионни договори.

РАЗДЕЛ XV

ЗАЩИТА НА АВТОРСКИТЕ ПРАВА

64. Политиката на Община Септември за защита на авторските права е изцяло съобразена със Закона за авторското право и сродните му права.

РАЗДЕЛ XVI

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

65. Политиката на Община Септември за защита на личните данни е изцяло съобразена със Закона за защита на личните данни.

РАЗДЕЛ XVII

ЗАКЛЮЧЕНИЕ

66. Настоящата политика се предоставя на трети страни, които имат достъп до информацията и системите на организацията, с цел запознаване и недопускане на инциденти, които да поставят в риск сигурността.
67. Настоящата политика се преразглежда редовно, с цел гарантиране на нейната уместност, адекватност и ефективност регулярно, но не по-малко от веднъж годишно и в случай на закони, организационни и технически промени.
68. Всеки служител, който прецени, че има злоупотреба с настоящата политика, уведомява незабавно служителя по мрежова и информационна сигурност.
69. Всеки служител, за когото е установено, че е нарушил тази политика, подлежи на дисциплинарна отговорност.
70. Ролите във връзка с отговорностите по провеждане на политиката по информационна сигурност се разпределят за изпълнение от конкретни длъжностни лица чрез правила, заповеди, допълнение на длъжностни характеристики или по друг подходящ начин.
71. Служителите на Община Септември се задължават да спазват всички вътрешни актове, издадени във връзка с информационната сигурност.
72. Постоянно действащата работна група изготвя, а кмета одобрява план за действие за постигане на заложените в политиката цели чрез определяне срокове, отговорни структурни звена и/или длъжностни лица.
73. Настоящата политика е утвърдена със Заповед №.....2079/09.12209..... и влиза в сила след нейното приемане.

ДЕКЛАРАЦИЯ ЗА КОНФИДЕНЦИАЛНОСТ

От:, в качеството на упълномощен представител на ..., със седалище и адрес на управление: град ..., ул. "... " № ..., ЕИК ..., представлявано от, ИЗПЪЛНИТЕЛ по договор за ... с ОБЩИНА СЕПТЕМВРИ, гр. Септември, ул. "Ал. Стамболийски" № 37а, БУЛСТАТ 000351825, представлявана от, като ВЪЗЛОЖИТЕЛ

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

1. Се задължавам да не разгласявам конфиденциална информация, получена от ВЪЗЛОЖИТЕЛЯ, станала ми известна в процеса на работата ми по изпълнението на Договора.
2. Конфиденциална информация по смисъла на настоящата Декларация е всяка информация, получена в писмен, устен или електронен вид, която се обработва в Сметна палата, включително информация относно лични данни, собственост, сделки, финансовото състояние и други за всички лица, за които се отнася тази информация.
3. Разгласяване на конфиденциална информация по смисъла на настоящата Декларация представлява всякакъв вид устно или писмено изявление, предаване на информация на хартиен, електронен или друг носител, включително по поща, факс или електронна поща, както и всякакъв друг начин на разгласяване на информация, в това число чрез средствата за масово осведомяване, печатните издания или Интернет.
4. Задължението за запазване на конфиденциалност има действие от датата на действие на договора и е без ограничение във времето.
5. Задължавам се да пазя конфиденциалната информация добросъвестно, за да предпазя разпространяването и публикуването ѝ от лица, които нямат правото да я разпространяват и публикуват.
6. Задължението за запазване на конфиденциалност няма да се прилага по отношение на информация, която е предадена по искане на компетентен орган, както и по отношение на информация, която е била публично оповестена или е била придобита от трети лица.
7. Задължавам се да върна на ВЪЗЛОЖИТЕЛЯ всички предоставени ми от него хартиени и/или електронни документи, предоставени ми по повод изпълнение на задължения по Договора.

Декларатор:

(трите имена, длъжност, подпис)