НАЦИОНАЛЕН STEM ЦЕНТЪР
1113 гр. София, бул. Драган Цанков, 21А, тел.02/ 873-83-57

УТВЪРДИЛ:

КАЛОЯН ЙОРДАНОВ
ДИРЕКТОР

В сила от 01.11.2021г.

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

В НАЦИОНАЛЕН STEM ЦЕНТЪР

Ноември 2021 г.

I.ВЪВЕДЕНИЕ

Чл.1. Настоящите правила за мрежова и информационна сигурност на Национален STEM център задават системата от мерки, които гарантират достъпност, интегритет и конфиденциалност на информацията по време на целия й жизнен цикъл (създаване, обработване, съхранение, пренасяне и унищожение) във и чрез информационните и комуникационните системи на Национален STEM център.

Чл.2. Тези правила определят отговорностите, задълженията и правата на потребителите на компютърната среда в Национален СТЕМ център /НСЦ/.

Чл.3. Нормативна база, въз основа на която са разработени правилата

1. Закон за електронното управление, в сила от 13.06.2008 г., обн. ДВ бр. 46 от 12 Юни 2007 г., доп. ДВ бр. 98 от 9 Декември 2016 г.

2. Закон за киберсигурност, обн. ДВ бр. 94 от 13 ноември 2018 г.

3. Постановление № 186 от 19 юли 2019 г. за приемане на Наредба за минималните изисквания за мрежова и информационна сигурност.

II.ОБЩИ ПОЛОЖЕНИЯ

Чл.4. Директорът на Национален STEM център има следните права и отговорности:

1. Носи пряка отговорност за мрежовата и информационната сигурност в обхвата на Наредба за минималните изисквания за мрежова и информационна сигурност;

2. Създава условия за прилагане на комплексна система от мерки за управление на тази сигурност; системата обхваща всички области на сигурност, които засягат мрежовата и информационната сигурност на информационните и комуникационните системи;

3. Осигурява необходимите ресурси за прилагане на пропорционални и адекватни на рисковете организационни, технически и технологични мерки, гарантиращи високо ниво на мрежова и информационна сигурност;

4. Упражнява контрол върху нивото на мрежовата и информацинната сигурност чрез провеждане минимум веднъж в годината на периодичен преглед на мрежовата и информационната сигурност и на адекватността на предприетите мерки;

5. Определя, документира и налага отговорности по изпълнението, контрола и информираността за всички процеси и дейности, свързани с развитието, поддръжката и

експлоатацията на информационните и комуникационните системи;

6 Определя със заповед служител по сигурността на информацията.

Чл.5. Служителя по сигурността на информацията на НСЦ има следните права и отговорности:

1. Ръководи дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност и целите, заложени в политиката на Национален STEM център по чл. 4 от Наредбата за минималните изисквания за мрежова и информационна сигурност;

2. Участва в изготвянето на политиките и документираната информация;

3. Следи за спазването на вътрешните правила по смисъла на чл. 5, ал. 1, т. 6 и прилагането на законите, подзаконовите нормативни актове, стандартите, политиките и правилата за мрежовата и информационната сигурност;

4. Консултира директора на Национален STEM център във връзка с информационната сигурност;

5. Ръководи периодичните оценки на рисковете за мрежовата и информационната сигурност;

6. Периодично (не по-малко от веднъж в годината) изготвя доклади за състоянието на мрежовата и информационната сигурност в центъра и ги представя на директора;

7. Координира обученията, свързани с мрежовата и информационната сигурност;

8. Организира проверки за актуалността на плановете за справяне с инцидентите и плановете за действия в случай на аварии, природни бедствия или други форсмажорни обстоятелства. Анализира резултатите от тях и организира изменение на плановете, ако е необходимо;

9. Поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност;

10. Следи за акуратното водене на регистъра на инцидентите;

11. Уведомява за инциденти съответния секторен екип за реагиране на инциденти с компютърната сигурност в съответствие с изискването на чл. 31, ал. 1 от Наредбата за минималните изисквания за мрежова и информационна сигурност (уведомяване за инциденти) от Наредбата за минималните изисквания за мрежова и информационна

сигурност;

12. Организира анализ на инцидентите с мрежовата и информационната сигурност за откриване на причините за тях и предприемане на мерки за отстраняването им с цел намаляване на еднотипните инциденти и намаляване на загубите от тях.

13. Следи за актуализиране на използвания софтуер и фърмуер;

14. Следи за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлага адекватни мерки за противодействието им;

15. Организира тестове за откриване на уязвимости в информационните и комуникационните системи и предлага мерки за отстраняването им;

16. Организира и сътрудничи при провеждането на одити, проверки и анкети и при изпращането на резултатите от тях на съответния национален компетентен орган;

17. Предлага санкции за лицата, нарушили мерките за мрежовата и информационната сигурност.

Чл.6. Потребител на компютърната и информационната среда на НСЦ е всеки служител по трудово правоотношение.

Чл.7. Достъпът на потребителите до информационните системи се определя от директора на НСЦ

Чл.8. При проблеми във връзка с използването на компютърната техника и информационните системи, потребителят подава сигнал към фирмата поддържаща компютрите.

Чл.9. На компютрите, включени в локалната мрежа на Национален STEM център се правят типови инсталации на програмни продукти, описани в приложение №1.

Чл.10. Допълнителен софтуер се инсталира само след доказана служебна необходимост и след разглеждане на наличието на лицензи, авторски права и съвместимост с останалите приложения.

III. ПРАВА НА СЛУЖИТЕЛИТЕ

Чл.11. Всеки служител в зависимост от необходимостта за изпълнение на трудовото си задължение има право на:

1. Оборудване с персонален компютър работно място с инсталиран стандартен софтуер и всички неободими специфични програми, необходими за изпълнението на служебните ангажименти.

2. Възможност за ползване на локален или мрежов принтер;

3. Възможност за ползване на друга периферна техника, необходима за изпълнение на служебните задължения;

4. Достъп до Интернет при изпълнение на присъщите му служебни задължения или за други цели в интерес на Национален STEM център .

5. Използва интернет от регламентираните доставчици;

6. Обмен на компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните задължения и само със служителите;

7. Споделена директория на файловия сървър;

8. Достъп до адресираните към него документи в системата за документооборот, съобразно йерархията и функциите на изпълняваната длъжност и Правилника за организацията на документооборота в Национален STEM център .

9. Служебен е-майл адрес.

IV. ЗАДЪЛЖЕНИЕ НА СЛУЖИТЕЛИТЕ

Чл.12. На служителите се забранява:

1. Да осигурява достъп на външни лица за работа с персоналните компютри на центъра, с изключение на пълномощници на фирмите, обслужващи софтуерните продукти.

2. Да инсталира и размества компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства. Тези действия могат да се извършват само след съгласуване с директора.

3. Да внася и включва в локалната мрежа техника, която не е собственост на центъра;

4. Да инсталира или позволява на друго лице инсталирането на софтуер и хардуер на компютъра, освен на служител от дирекция „Информационни и комуникационни технологии“ на Министерството на образованието и науката;

5. Да прави опити за достъп до компютърна информация и бази данни, до които не са предоставени права, съобразно заеманата от служителя длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп;

6. Да използва преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на Национален STEM център, без знанието на служителя, отговарящ за сигурността на мрежовата и информационна сигурност;

7. Да променя настройките в хардуерния SETUP на компютъра (BIOS), системните настройки на операционната система, потребителския интерфейс и конфигурацията на компютъра.

8. Да ограничава по какъвто и да е начин работата на антивирусната защита.

9. Да използва Интернет за нарушаване на правата върху интелектуалната собственост чрез разпространение на информация, програмно осигуряване или документи със защитени авторски права;

10. Да генерира ненужен трафик от съобщения, да разпространява данни или програми, които могат да нарушат работата на останалите потребители, да изпраща големи файлове или множество файлове в некомпресиран вид.

11. Да ползва мрежата за каквито и да било извънслужебни цели (личен бизнес, рекламни цели);

12. Да прави или подпомага опити за неоторизиран достъп до мрежови ресурси, информация и бази данни, компютри и други устройства на центъра или други звена на държавната администрация (използване на чуждо потребителско име/парола; физически достъп до компютър, на който в момента е оторизиран друг потребител; злонамерено възползване от съществуващи пропуски в операционните системи, протоколите или приложния софтуер, позволяващи неоторизиран достъп, както и чрез други средства и похвати).

13. Да стартира изпълними модули, програми и макроси, включени в документни файлове, получени по електронната поща, независимо от това кой и защо ги праща.

14. Да инсталира и използва програмни продукти или приложения за отдалечен достъп до работния плот и файловете в компютъра на работното му място без знанието и разрешението на служителя, отговарящ за сигурността на информацията.

15. Да свързва компютри едновременно в мрежата на Национален STEM център и в други мрежи, в противоречие с изискванията на Закона за електронното управление и Наредбата за минималните изисквания за мрежова и информационна сигурност (ДВ БР. 59/2019 г.).

16. Да инсталира и използва комуникатори (Skype и други подобни), осигуряващи достъп извън рамките на компютърната мрежа на Центъра 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 Национален STEM център ;

17. Да съхранява на сървъра лични файлове с текст, изображения, видео и аудио.

V. ЗАДЪЛЖЕНИЕ НА СЛУЖИТЕЛИТЕ ОТНОСНО ТЕХНИКАТА

Чл.13. Всеки служител работещ с поверена компютърна техника има следните задължение:

1. Всеки потребител отговаря за поверената му техника и е длъжен да я ползва с грижата на добър стопанин и да спазва инструкциите за експлоатация.

2. Компютърната техника се разполага от лицето, отговарящо за поддръжката, по оптимален начин, след съобразяване с техническите и материалните ресурси и възможности.

3. Промяна на местоположението на техниката става след разрешение на ръководителя и съгласуване с лицето по поддръжка, което извършва разкачване и след преместването, включване и настройка.

4. Включването на свързана компютърна конфигурация става задължително към един разклонител и към съответната електроинсталация. Не се включват други електрически

уреди (радиатори, електрически печки, климатици и т.н.) към контактите или разклонителите, захранващи компютърната техника;

5. Не се поставят книги, хартия, дрехи, саксии с цветя и други вещи в близост и върху устройствата.

6. Не се допуска попадане на чужди тела и течности в устройствата. В близост до устройствата и върху тях не се слагат съдове с напитки и хранителни продукти, лесно запалими материали и течности. Не се поставят устройства по первазите на прозорците и други рискови места. При възникване на инцидент или повреда, потребителят веднага следва да изключи устройството от електрическото захранване и да уведоми незабавно служителя по поддръжката на компютърната техника и служителя по сигурността на информацията.

7. Потребителят трябва да поддържа техниката, с която работи, чиста. За почистване не трябва да се използва спирт и други агресивни препарати, които могат да повредят повърхностите. Особено внимание да се обръща на екраните на мониторите - за целта може да се използва мека кърпа (която не оставя власинки), след като устройствата се изключат от електрическото захранване;

8. Не се допуска прегъване, опъване и стъпване върху свързващите кабели.

VI. ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ ОТНОСНО ПРЕНОСИМИТЕ УСТРОЙСТВА И ИНФОРМАЦИОННИ СРЕДСТВА

Чл.14. Всеки служител ползващ преносими лаптопи е длъжен:

1. Да ги защитава от кражба и загуба - особено в транспортни средства, хотелски стаи, зали за конференции и места за срещи и други обществени места.

2. Да съобразява разположението си с цел да избегне наблюдение на екрана от неупълномощени лица;

3. Да използват заключващи и криптиращи методи за защита на информацията.

4. Да отчита риска при работа в незащитена среда и възможността за попадане на злонамерен софтуер или прихващане/подслушване на съобщения.

5. Да поддържа актуална версия на базата на антивирусната програма.

6. Използване на служебна информация чрез отдалечен достъп през обществена мрежа да се извършва само и след успешна идентификация и автентификация на потребителя;

7. Да прави редовно резервни копия на информацията, намираща се върху преносимите устройства върху друг носител и да не оставя файлове в преносимото устройство след приключване на задачата.

8.

VII. ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ ОТНОСНО ПАРОЛИТЕ

Чл.15. Всички служители ползващи компютърни конфигурации имат следните права и задължения относно използването на пароли:

1. Служителят получава различни потребителски имена и пароли за достъп до различните мрежови ресурси.
2. Не се използва една и съща парола за достъп до различни ресурси.
3. Служителят е длъжен да смени незабавно предоставените му служебни пароли за достъп.
4. Служителят трябва да използва само своето потребителско име и лична парола.
5. Служителят не трябва да предоставя потребителското си име и парола на друго лице.
6. Парола, станала известна на неоторизирано лице, трябва да се смени незабавно и да се уведоми прекия ръководител
7. Служителят трябва периодично (на всеки 3 месеца) да сменя паролата си.
8. Паролата трябва да е с дължина не по-малко от 12 символа – и да съдържа задължително малки и големи букви, цифри и специални символи.
9. **Пример**

Неправилни пароли: 63636363, ivanpetrov, qwerty,

Правилна 12 символна парола: ***Pepi3456789****

10. Списъците с паролите за достъп се съхраняват на защитено място (сейф или заключен шкаф).

VIII. ЗАДЪЛЖЕНИЕ НА СЛУЖИТЕЛИТЕ ОТНОСНО СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Чл.16. Потребителят не трябва да отваря файлове от външен носител преди да са проверени за наличие на вируси.

Чл.17. Всеки потребител е самостоятелно отговорен за съхранението и защитата на файловете и информацията, съхранявани на локалния твърд диск на компютъра, предоставен му за служебно ползване, както и на преносимите устройства.

Чл.18. Да не съхраняват файлове с документация на Desktop на работното място, както и върху преносимите устройства, собственост на Центъра.

Чл.19. При напускане на работното място да заключва компютъра си, а след приключване на работния ден:

1. Да изключи компютъра;
2. Да прибира своевременно разпечатаните документи от принтерите. ,
3. Да не оставя документи в скенерите.
4. Да не оставя документи върху бюрото или работната маса, след приключване на работа с тях или когато напуска помещението.

Чл.20. При промяна или прекратяване на служебните/трудови правоотношения потребителят трябва да предаде на прекия си ръководител цялата служебна информация на хартиен носител или/и в електронен вид, с която е работил, както и всички пароли за защитените файлове.

Чл.21. Потребителят е длъжен да уведоми веднага служителя по информационна сигурност за забелязани нарушения на посочените в тази инструкция правила или за действия, които са заплаха за сигурността на информацията (неоторизиран физически или логически достъп, неправилно съхранение на документи, нарушение на работни процедури и инструкции, повреда или грешки на техническо оборудване и т.н.).

Чл.22. Потребителите участват задължително в периодично организираните от ръководството обучения за опазване мрежовата и информационна сигурност и техните отговорности за нея.

Чл.23. При прекратяване на основанията за ползване на потребителски права, e-mail адресът се блокира за достъп от потребителя. По искане на служителя по сигурността на информацията се създава възможност за пренасочване на получаваните съобщения от блокирания адрес към друг служебен адрес за срок не по-дълъг от 1 месец. След този срок e-mail адресът се заличава. Изключения от това правило се правят само след изрично писмено разпореждане на директора на Национален STEM център преди изтичане на срока за заличаване.

IX. РЕГИСТЪР НА ИНЦИДЕНТИ

Чл.24. Национален STEM център поддържа регистър на инцидентите, в който се отбелязва време на възникване и време на разрешаване на инцидента, как е разрешен и от кого. Това дава възможност да се направи анализ за откриване на причините за инцидентите, за да се отстранят, както и чрез натрупаната информация ще спомогне за по-бързото разрешаване на подобни инциденти, появяващи се в последствие, т.е. ще се намали времето за реакция, времето на престой и броя на инцидентите.

Чл.25. В случай на смущения в работата на информационните системи се докладва на лицето, отговарящо за сигуростта на информацията. Ако се установи, че става въпрос за заплахи, които могат да бъдат използвани за атаки, идващи от Интернет, се предприемат мерки за уведомяване на екипа за реагиране при инциденти с компютърната сигурност, създаден към ДАЕУ (контактни точки: 02 949 2212, 0878 908546, cert@govCERT.bg).

Чл.26. При инцидент с мрежовата и информационната сигурност, служителят по информационна сигурност на Национален STEM център уведомява съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите в сроковете, посочени в чл. 21, ал. 4 и 5 и чл. 22 от Закона за киберсигурност.

Чл.27. Регистърът с инциденти се поддържа от служител в Национален STEM център , определен със заповед на директора.

X. РАБОТА СЪС СОФТУЕРА

Чл.28. Списък на стандартния и специализирания софтуер, използван на работните места от Национален STEM център са описани в Прилижение №1

Чл.29. За всекидневната си работа потребителите – служители на Национален STEM център разполагат с лицензиран, предоставен от Министерството на образованието, софтуер.

Чл.30. За изпълнението на специфични дейности, свързани с изпълнението на конкретни задачи, на някои от работните места се инсталира локално и специализиран софтуер .

XI.РАБОТО С ЕЛЕКТРОННИ ПОДПИСИ

Чл.31. Работата с електронен подпис и електронно подписване на документи от упълномощените за това служители на Национален STEM център се извършва в съответствие с разпоредбите на Закона за електронното управление - Раздел II - Подаване на електронни документи, Раздел III - Приемане на електронни документи, Раздел IV - Изпращане и съхраняване на електронни документи.

Чл.32. Електронен подпис се закупува на всички служители, чиито задължения изискват ползването на такъв.

Чл.33. Отговорност за безопасното съхранение на смарт картата, флашпаметта или друг носител, както и ПИН кода се носи само и единствено от съответния служител.

Чл.34. Забранява се ползването на електронния подпис на определен служител от други лица.

XII. СПЕЦИФИЧНИ ПРАВИЛА ЗА РАБОТА С КОМПЮТРИ В НСЦ

Чл.35. Правила за работа с файлове са следните:

1. Всички електронни копия на документи в Центъра се създават на бланка на Национален STEM център за първа страница.

2. Потребителят периодично съхранява файловете, които обработва, за да предотврати загубата на данни от прекъсване на захранването или други непредвидени обстоятелства в специално създадени за целта индивидуални папки на сървъра;

3. Допустими файлови формати за работа в Национален STEM център са:

Поради спецификата на софтуера на служебните компютри, за текстови документи и електронни таблици се използват форматите на Microsoft Office:

1) „.doc", „.docx" за документи, подготвени с Microsoft Office , 2007 или 2010;

2) „.xls", „.xlsx" за таблици - Microsoft Office Excel 2003, 2007 или 2010;

3) „.ppt" ,".pptx" - за презентации в работен вид с MS PowerPoint.

4) Други, в зависимост от конкретните задачи:

5) „.pdf" или „.jpg" формат за изображения на сканирани документи;

6) „zip" или „rar" формат за архивиране на няколко документа, отнасящи се към обща тема (напр. отчет и приложения към него).

7) "fed" за документи разработени със Редактора на форми на АОП

8) .jpg, .jpeg, .eps,.png,.svg,.jpg,.tiff и др за графични изображения, като при сканиране на документите се използва по-ниска резолюция (100 – 150 dpi), черно-бял формат и файловете следва да се записват в оптимизиран формат - jpg или pdf за да има възможност за изпращането им по електронна поща.

9) .erf (Equa Report File) формат за съхраняване на отчети от Еква равнение.

4. Забранени за работа и съхранение файлови формати на изтеглени или копирани изпълними (инсталационни) файлове

Забранява се съхраняването и използването на служебните компютри на файлове със следните формати:

.action, .apk, .app, .bat, .bin, .cmd, .com, .command, .cpl, .csh, .exe, .gadget, .inf, .inf1, .ins, .inx, .ipa, .isu, .job, .jse, .ksh, .lnk, .msc, .msi, .msp, .mst, .osx, .out, .paf, .pif, .prg, .ps1, .reg, .rgs, .run, .scr, .sct, .shb, .shs, .u3p, .vb, .vbe, .vbs, .vbscript, .workflow, .ws, .wsf, .wsh и др.

5. Работа с получени от външен източник архиви (zip, rar, 7z)

1) Потребителят е длъжен при получаване от какъвто и да е външен източник на архиви – прикачени файлове към електронно съобщение, архиви на външен носител (USB-памет, външен твърд диск и т.н.), свалени от официални страници в Интернет, задължително да ги сканира с антивирусната си програма преди да пристъпи към разкомпресиране на съдържанието.

2) При отчитане на опасност при работа на антивирусната програма незабавно се прекратява работа и се сигнализира лицето, отговарящо за поддръжката на компютрите.

Чл.36. Работа с електронна поща

1. Процедури при работа с електронната поща

Електронната поща е един от най-опасните източници за внедряване на зловреден софтуер както на отделното работно място, така и в цялата мрежа.

При проверка на електронната поща за нови съобщения:

1) Стартира се пощенския клиент на работното място

2) Прави се оглед на новите получени съобщения, без все още да се отваря нищо.

3) Съмнителните съобщения се игнорират и се съобщават по установения ред на служителя по поддръжка на компютърната техника.

4) За съобщенията, за които се счита, че имат отношение към работата, се проверява източника.

Пример:

Уведомително съобщение, привидно изпратено от НАП, при проверка на адреса на подателя, се оказва, че не е изпратено от техни пощенски сървъри (вместо от име@nra.bg е изпратено от име@nra.cn – примерен адрес от Китай)

5) При установяване, че към вече провереното за достоверност на подателя съобщение има прикачен файл, потребителят проверява разширението на файла и ако то е включено в примерния списък на забранени файлови формати или е

непознато за него, незабавно прекратява работа и съобщава по установения ред на лицето, отговарящо за сигурността на информацията.

6) Потребителят сваля прикачените файлове в нарочна папка на локалната машина, определена от служителя по поддръжка на компютърната техника и задължително ги сканира ръчно с антивирусната си програма.

XIII. РАБОТА С АВТОМАТИЗИРАНА ИНФОРМАЦИОННА СИСТЕМА ЗА ДОКУМЕНТООБОРОТ

Чл. 37. Служителите на Национален STEM център използват система за управление на документооборота и работния поток „EVENTIS R7". Системата за документооборот е инсталирана на сървъра на МОН, а Национален STEM център е ползвател.

Чл.38. Служителите в Национален STEM център имат достъп до системата за документооборот като:

1. администратори в системата за документооборот е директора
2. потребители в системата за документооборот – всички останали служители .

Чл.39 Потребителски имена и достъп се задават от администратора, като:

1. Всеки потребител се идентифицира с потребителско име и парола, които се предоставят от администратора.

2. Достъпът до информацията в системата за документооборот е персонализиран – всеки потребител вижда само документите, които имат отношение към неговата работа на база мястото му в организационата структура и ролята, която изпълнява.

Приложение №1

Списък на стандартния и специализирания софтуер,

използван на работните места Национален STEM център

1. Windows 10
2. Офис пакет за Windows 10
3. Счетоводен софтуер - Микроинвес -"Делта -про", "Заплати";
4. Софтуер за работна заплата и граждански договори "Омега тим"
5. Електронно банкиране на банки ДСК и ОББ
6. Деловен софтуер "Евентис"
8. Счетоводен софтуер "Еква-равнение"
9. Електронни подписи на "B-trust"
10. Архивираща програма "7-zip"
11. Софтуер за принтери на CANON,
12. Сканиращ софтуер на Microsoft corporation
13. Skype
14. Microsoft Silverlight
15. Adobe Acrobat Reader DC
16. Zoom
17. Vaiber
18. Windows 7
19. ЕСТИ -/Единна система за туристическа информация/
20. Електронни услуги на НАП и НОЙ
21. Софтуер за копиране и периферна техника
22. Други драйвери