



УТВЪРЖДАВАМ

Изпълнителен директор:

/Галина Деликирова/

ПРАВИЛА

ЗА РАБОТА НА СЛУЖИТЕЛИТЕ

В ИНФОРМАЦИОННА СИСТЕМА И В ИНТЕРНЕТ

Информационната система на Фондация „Надежда” - Кърджали е изключително важна и трябва да бъде защитена от промяна или унищожаване вследствие на злонамерен програмен код. В основата на превенцията срещу вируси е информираността на служителите за методите на защита по отношение на сигурността.

ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ:

1. Всеки софтуерен продукт /в това число снимки, клипове и т.н/, получен чрез изтегляне от интернет, трябва да се третира като „ненадежден“ и да се подлага на проверка за вируси. Когато се теглят файлове от интернет, те следва да се разглеждат като подозрителни и да не се стартират или използват по никакъв начин, докато не бъдат сканирани за вируси.

2. Внимателно използване на електронната поща, която крие голям риск за навлизането на вирус в мрежата чрез фишинг - фалшиви

електронни писма, които изглеждат сякаш са написани от оригиналния източник, и Ви насочват да отговорите или да посетите фалшив сайт.

3. Да не се инсталира на служебните компютри или мрежи никакъв софтуер.

4. Редовно сканиране на компютъра с антивирусен софтуер.

5. Редовно преглеждане на меню History на антивирусната програма, където се отчитат потенциални заплахи. Ако служителят забележи такава, веднага уведомява системния администратор.

6. Редовно почистване на ФАЙЛОВЕТЕ от папки Temp 1 и 2 на Desktop.

7. Редовно почистване кеша на интернет и хронологията на браузъра, който се използва.

8. Приложения и раздели в уеб браузъра, които не се използват се затварят.

9. Нежелателно е абониране за новинарски групи в интернет, мейлинг листи и др.

10. Нежелателно е посещаването на сайтове със съмнително съдържание, фалшиви сайтове, реклами, изскачащите прозорци, фишинг;

11. Стандартно защитения с парола скрийнсейвър следва да се активира, когато персоналният компютър е оставен без надзор.

12. Лица, които не са служители на библиотеката нямат право на достъп до компютърните системи и мрежи. Той се ограничава единствено до информацията, която е от значение за третата страна.

13. Достъпването на безжичната мрежа на библиотеката с лични устройства да става след наличие на антивирусен софтуер на тези устройства.

14. Файловете, пренасяни на флаш памет или друг носител, задължително се сканират с антивирусна програма

15. Уеб браузърите, операционната система и софтуера се поддържат винаги актуални.

16. Посещават се само сайтове със сертификат за защита S / <https://>, а не <http://>. Сертификатът гарантира, че целият процес на кодиране остава законен и безопасен.

ЗАЩИТА И СЪХРАНЕНИЕ НА ДАННИ

- Данните се резервират като се отчита критичността им за работата, както и времето, усилията и средствата, вложени за повторното им създаване или възстановяване.

РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ, СВЪРЗАНИ СЪС СИГУРНОСТТА

Инцидент, свързан със сигурността е всяко събитие, при което има или би могло да възникне нарушение на политиката и процедурите за сигурност или което е довело до загуба или повреждане на активите на библиотеката.

1. Инцидентите, свързани със сигурността, задължително се докладват възможно най-бързо на системния администратор и директора.

2. При инцидент се изключва LAN кабела от съмнителния компютър.

3. Служителите носят отговорност за:

- използване на интернет, представляващо заплаха за сигурността на информационната система на библиотеката
- правилното използване и опазване на поверените им ИТ ресурси;
- изпълнение на всички указания и процедури за защита на информационната система на библиотеката

4. Служителите търпят санкции за поведение в интернет, което е поставило под заплаха сигурността на информационната система на библиотеката.

ОЦЕНКА НА РИСКА И ПРЕГЛЕД НА СИГУРНОСТТА

Системният администратор периодично извършва оценка на риска и преглед на сигурността и предлага , ако това е необходимо, на директора промени в настоящите Правила.

Системен администратор:

/ Г. Деликирова/

20.01.2020 г.