Основно училище "Стефан Караджа"
гр. Варна, район Приморски ул. "Братя Бъкстон" № 11, 052/635967,school@stefankaradja.com

Инструкция за използването на информационните системи от служителите

Раздел I. Общи положения

Чл. 1. (1) Инструкцията за използване на информационните системи информира педагогическите специалисти и непедагогическия персонал за правата и задълженията им по отношение на използването нейното приложение и използване.

(2) Инструкцията определя правилата за използване на информацията за вътрешна и външна комуникация, за предоставяне на услуги на родители и учители, за администриране, свързано с учебно-възпитателния процес, а също така е средство за извършване на проучвания и обмяна на информация.

(3) Достъпът до данните в локалната мрежа и ползването на програмните продукти на институцията от педагогическите специалисти и непедагогическия персонал е необходимо с оглед ефективното изпълнение на отговорностите и задълженията.

Чл. 2. Информационните технологии включват локалните мрежи, интернет, електронната поща и всички програмни продукти, които институцията притежава и ползва.

Чл. 3. Инструкцията дава указания за начина на употреба от от педагогическите специалисти и непедагогическия персонал на информационните технологии, насърчава ползването им с цел увеличаване на продуктивността и ефективността на работата.

Чл. 4. (1) Определеният заместник-директор, ръководителят на направление „Информационни и комуникационни технологии“/специалистът по IT технологии в институцията са отговорни за цялостната дейност на информационните технологии и за подпомагането работата на служителите на институцията с тях.

(2) При съмнение за нарушение на сигурността на личните данни, лицето, което е установило несъответствието (случайно или неправомерно унищожаване на лични данни, загуба, промяна, неразрешено разкриване или нерегламентиран достъп, незабавно уведомява лицата по ал. 1 и определения служител по защита на личните данни за предприемане на действия по прилагане на Инструкцията за действие при пробив в сигурността.

Чл. 5. Служителите в институцията са задължени да спазват правилата, определени с настоящата Инструкция.

Чл. 6. Всички компютърни програмни продукти и информация, създадена и съхранена от служителите, са собственост на институцията.

Чл. 7. Служителите в институцията нямат право да вземат програмните продукти с цел инсталирането им на домашните им компютри и преносими устройства, с изключение на електронните учебници и създадените за он-лайн обучение софтуери.

Чл. 8. При напускане на институцията служителите нямат право да копират или унищожават файлове с данни, които са създадени във връзка с тяхната работа.

Раздел II. Контрол върху работата с информационните технологии

Чл. 9. (1) Ръководството на институцията има право да контролира ползването на програмните продукти, електронната поща, Интернет и базите данни, създадени от служителите в институцията.

(2) Ръководството на институцията, включително и определеното длъжностно лице по защита на личните данни, имат право да проверява изцяло служебните компютри, предоставени за учебни цели на служителите в институцията, както и техниката, която ползват учители и служители във връзка с изпълнение на служебните им задължения.

Раздел III. Конфиденциалност

Чл. 10. Резултатите от извършения контрол върху работата с информационните технологии на институцията се считат за конфиденциални и не се разгласяват от ръководството.

Раздел IV. Допустимо ползване на информационните технологии за лични цели

Чл. 11. Учебните информационни системи са предназначени за ползване при изпълняване на служебните задължения на служителите.

Чл. 12. Тези системи могат да се ползват и за лични цели при следните условия:

1. Това е инцидентно, рядко и за кратко време.
2. Не е по време на работа, а е в извънработно време.
3. Това не пречи на работата на останалите служители. В това число се включват дейности, които могат да доведат до конфликт на интереси.
4. Това не води до допълнителни разходи за институцията.

Раздел V. Забрани за ползване на информационните технологии

Чл. 13. Забранява се ползването на компютърните и информационните системи на институцията в следните случаи:

1. Заобикаляне на системите за сигурност, с цел разрушаване или намаляване сигурността на учебната локална мрежа или бази данни.
2. Ползване на информационните ресурси за извършване на нерегламентирана дейност.
3. Използване на ресурсите за подпомагане дейността на външни организации, техните продукти, услуги или бизнес практика, с цел облага.
4. Електронна поща на институцията не може да се ползва за комерсиални лични цели, религиозни цели или да се подпомага бизнес, който не е свързан с дейността на институцията.
5. Ползването на компютърните системи за политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат.
6. Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност. Всички електронни писма, пращани от служители на институцията трябва да са лично подписани и да са до точно определен брой адресати, които са дали съгласие за използване на електрлонния им адрес.
7. Свалянето от Интернет на аудио и видео файлове и други.
8. Сваляне и инсталиране на компютърни програми от Интернет без разрешение на компютърните специалисти.

9. Копиране на лицензираните компютърни програми на институцията с цел лична употреба.

Раздел VI. Разкриване на информация

Чл. 14. (1) Неоторизираното разкриване на служебна информация може да доведе до негативни последици за институцията и накърняване на нейния имидж и репутация.

(2) Служител, който е копирал и използвал информация от локалната мрежа на институцията за лична изгода или за да причини вреда на институцията, носи съответната дисциплинарна и имуществена отговорност по КТ.

Раздел VII. Антивирусна защита

Чл. 15. (1) Компютърните вируси са голяма заплаха за всички потребители на IT услуги и служителите трябва да имат необходимите знания как вирусите се разпространяват, каква вреда могат да нанесат и как да се предпазват от тях.

(2) Компютърният вирус е компютърна програма, която се задейства на даден компютър и се разпространява към другите дискове и програми, които са в контакт със заразения компютър.

(3) Вирусът може да причини блокиране на компютъра, да промени бази данни, да направи някои данни невъзможни за ползване и даже да форматира диск и така да се загуби цялата информация на тях.

Раздел VIII. Организация на защитата от вируси

Чл. 16. (1) IT специалиста на институцията носи пълната отговорност за избирането и инсталирането на антивирусната програма, както и за нейната актуализация на всеки индивидуален компютър. Служителите също трябва да следят дали тяхната антивирусна програма се осъвременява поне веднъж седмично с най-новата версия.

(2) Служителите трябва да приемат всяко съобщение за вирус изключително сериозно и да следват вътрешните процедури за реакция в такъв случай.

(3) Преднамереното разпространяване на данни, за които служителят знае, че са заразени е нарушение на служебните задължения, което се санкционира по дисциплинарен ред.

(4) В случай на вирусна атака служителят трябва незабавно да информира IT специалист без да предприема никакви действия самостоятелно.

(5) На служителите е разрешено да свалят файлове от външни източници на мрежата на институцията във връзка с тяхната работа. Не е разрешено на служителите да се инсталират програмни продукти без предварителното разрешение на IT специалиста, тъй като има опасност от заразяване с вируси.

(6) Входящата електронна поща трябва да се третира с особено внимание поради потенциалната възможност да е заразена с вируси. Отварянето на приложения да се прави само след предварителното им сканиране с антивирусна програма.

(7) Електронни писма, получени от неизвестни податели трябва да се изтриват и в никакъв случай да не се отварят файлове, прикачени към тях.

(8) Файлове, получени от неизвестни податели трябва да се трият без да се отварят.

(9) Ползването на външни носители (дискове, външна памет и др.) на информация е допустимо само след предварителното им сканиране с антивирусна програма.

Раздел IX. Архивиране на информацията

Чл. 17. (1) Сривовете в компютърното оборудване, вирусите, случайното изтриване на файлове могат да причинят загуба на данни, поради което е необходимо информацията във всяка компютърна система да бъде архивирана.

(2) Целта на архивирането и възстановяването е да се възстанови работата възможно най-бързо в случай на прекъсване по технически причини. По този начин се минимизират възможните проблеми и загуби.

(3) Служителите в институцията, съгласувайки с IT специалиста, трябва да имат адекватна система за архивиране на данните от своята работа на технически носители (дискове, USB и др.).

(4) Честотата на архивирането се определя от директора в писмена процедура и зависи от броя транзакции и тяхната значимост за системата.

(5) Задължително архив (архивиране на файлове) се прави веднъж месечно.

Раздел X. Достъп и пароли

Чл. 18. (1) Служителите получават достъп до локалната мрежа и до всички програми, необходими за изпълнение на служебните им задължения.

(2) Достъпът до дадена програма се дава на конкретен служител и не може да се прехвърля на друг.

(3) Служителите трябва да пазят своите лични пароли в тайна.

Чл. 19. Когато даден продукт изисква парола трябва да спазват следните правила:

1. служителите трябва да променят първоначалната парола (обикновено генерирана от програмния продукт) като измислят своя индивидуална при първото влизане в съответната информационна система;
2. паролите трябва да са с не по-малко от 5 знака;
3. паролите трябва лесно да се помнят, за да не се налага да бъдат записвани на хартия;
4. паролите не трябва да са лесни за отгатване от колегите;
5. паролите не трябва да се споделят с колеги или други познат;
6. паролите не трябва да се записват на хартия и да се оставят на работното място;
7. ако е необходимо паролите могат да се сменят на определена честота (всеки 3, 6, 12 месеца);
8. при 3 неуспешни опита за влизане в дадена програма достъпът може да бъде блокиран;
9. при периодична промяна на паролата не трябва да се използват вече използвани пароли;
10. системите не трябва да позволяват един и същи потребител да се включи в няколко компютъра едновременно с една и съща парола.

Чл. 20. Ако забравят своята парола служителите трябва незабавно да уведомят оторизирания помощник директор и да се свържат с IT специалист.

Раздел XI. Интернет

Чл. 21. (1) Ръководството насърчава ползването на Интернет от служителите за обмяна на информация, извършване на проучвания и събиране на данни във връзка с дейността им.

(2) Заместник-директорите и други оторизирани длъжностни лица отговарят за уместната употреба на Интернет от служителите на институцията.

(3) Свалянето от Интернет на аудио или видео файлове е забранено. Не е разрешено и свалянето на програмни продукти от Интернет без предварителното одобрение на компютърен специалист.

Раздел XII. Електронна поща

Чл. 22. (1) Електронната поща на институцията не може да се ползва за комерсиални цели, религиозни цели или да се подпомага бизнес, който не е свързан с дейността на институцията.

(2) Ползването на електронната поща за политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат също не се позволява.

(3) Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност се забранява. Всички електронни писма, изпращани от служителите трябва да са лично подписани.

(4) Неформалните съобщения, които не са от официален характер трябва да се трият от пощата, за да не се товарят сървърите на институцията.

(5) Всички електронни писма и важни съобщения, които имат отношение към дейността на училището, трябва да се принтират и представят за завеждане с входящ номер в дневника за входяща кореспонденция от определеното длъжностно лице, като екземпляр се съхранява в съответние класьор и в електронната поща.

(6) Служителите трябва да проверяват внимателно точния адрес на получателите на официални писма, особено такива с прикачени файлове, за да не се допусне получаване на информация от чужди лица.

Раздел XIII. Лице за контакт

Чл. 23. Всички технически въпроси във връзка с работата на компютърните системи се насочват към IT специалистиа на институцията или към друго лице, определено от директора.

Допълнителни разпоредби

§ 1. При извършване на самооценката на вътрешните контроли следва да се направи анализ и оценка на риска на критичните информационни системи в институцията.

§ 2. Целта е да е идентифицират най-важните компоненти (оборудване, програми, бази данни), заплахата за тяхната повреда или загуба, последиците от това за дейността на институцията налични контроли за да се предотвратят потенциалните проблеми и допълнителни контроли, които са необходими за подобряване на системата.

§ 3. Оценката на риска обхваща извършеното, както и моментното състояние, мерките за подобряване на слабите места във вътрешните контроли, необходимите ресурси и остатъчния риск за институцията, който контролите няма как да елиминират.

§ 4. При създаването на програмен продукт специално за нуждите на институцията е необходимо още при задаването на неговите параметри на доставчика да се заложат основните контролни функции, които този продукт трябва да има.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Инструкцията влиза в сила утвърждаването ѝ със Заповед РД-07-336 /10.12 2020г. на директора.

Ирена Динева Митева X
Директор СУ „Стефан Караджа“ - Варна