ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО МЕХАНОТЕХНИКА - СЛИВЕН

УТВЪРЖДАВАМ:.....

ТАТЯНА ПЕТКОВА

ДИРЕКТОР ПГМ

Заповед № РД-09-47/ 15.09.2021г.

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

2021г.

РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ

1. Настоящите правила са разработени и съответствие с Наредбата за минималните изисквания за мрежова и информационна сигурност от 26.01.2019 г. и имат за цел осигуряването на контрол и управление на работата на информационните системи в ПГМ гр. Сливен, общ.Сливен. В този смисъл понятието „информационна система“ се определя като съвкупност от компютърна и периферна техника, програмни продукти,данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми. Програмните продукти и бази данни могат да бъдат специфични или с общо предназначение.

2. Потребителите на информационни системи са задължени и отговорни с действията си да гарантират ефективното и ефикасно използване на системите.

3. 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 Наредбата за минималните изисквания за мрежова и информационна сигурност (ДВ, БР. 59 от 19.07.2019 г.)

РАЗДЕЛ II. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

4. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

- разделяне на потребителски от администраторски функции;
- установяване на нива и достъп до информация;
- регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;
- осъществяването на контрол.

5. Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили;

6. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез средствата на активна директория с конкретно потребителско име, осигурено от администратор/ оторизираното за това лице.

7. Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заеманата длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

8 Лицата, които обработват личи данни, използват уникални пароли с достатъчна сложност. които не се записват или съхраняват онлайн;

9. Всички пароли за достъп на системно ниво се променят периодично;

10. Всички носители на лични данни се съхраняват на безопасна и сигурни среда - в съответствие със спецификациите на производителите, в заключени шкафове, с ограничен и контролиран достъп.

11. За нарушение се считат следните действия:

- унищожаване на база данни или части от тях,
- повреждане на база данни или части от тях,

- променяне на база данни или части от тях.

12. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до злонамерен софтуер. Забранено е съобщаването на лична и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

13. След като повече не са необходими, носителите на информация се унищожават сигурно и безопасно за намаляване на риска от изтичане на чувствителна информация към неупълномощени лица. Физическото унищожаване на информационните носители става със счупване. Предварително се проверят, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

14. Събирането, подготовката на данните за интернет страницата и вписванията в нея се извършва от Стоянка Кръстева.

РАЗДЕЛ III. РАБОТНО МЯСТО

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

16. Всеки служител отговаря за целостта па компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място съобразно дадените му права.

17. Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него е въвеждането на потребителско име и парола;

18. Забранява се на външни лица да работят с персоналните компютри на училището, освен на 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 служител от училището.

19. След края на работния ден всеки служител задължително изключва компютъра, на който е работил;

20. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява служителят отговарящ за мрежовата и информационна сигурност, който му оказва съответна техническа помощ;

21. Забраняват се опити за достъп до компютърна информация и бази данни, за 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;

22. Инсталиране и разместване на компютърни конфигурации на части от тях. на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства се извършва само от администратор/ или от оторизирано за това лице.

23. Служителите имат право да обменят компютърна информация само във връзки с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

24. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача, при спазване на принципа „необходимост да се знае.”

25. Достъпът до компютърна информация, бази данни на софтуер се управляват от администраторът/ оторизираното за това лице и извършва следните дейности: активират се съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата; настройва антивирусния софтуер за периодични сканирания на файловите системи на компютрите за вируси; проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер;

• при поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира служителят отговаряш за мрежовата и информационна сигурност.

РАЗДЕЛ V. СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

26. Администраторът/ оторизираното за това лице осигурява автоматизираното създаване на резервни копия на всички база данни и електронни документи.

27. Информацията, включително тази, съдържаща лични данни, се архивира по следния начин:

- архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг сървър/' компютър и да се продължи работният процес без чувствителна загуба на данни;
- резервните копия се съхраняват на носител, различен от този, на който са разположени данните или електронните документи.
- резервните копия периодично се изпитват чрез пробно възстановяване на данни.

РАЗДЕЛ VI. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в ПГМ – Сливен са длъжни да познават и спазват разпоредбите и тези правила.

§ 2. Контролът по спазване на правилата се осъществява от директора на училищата.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед на ефективността. При необходимост се допълват с мерки и процедури, които са целесъобразни н необходими с оглед защитата на информацията.

§ 4. Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност (в сила от 26.07.2019 г.) м влизат в сила след утвърждаването им от директора.

ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО МЕХАНОТЕХНИКА - СЛИВЕН

З А П О В Е Д

№ РД – 09 - 47 / 15.09.2021г.

На основание чл. 258, ал. 1 и чл. 259, ал. 1 от ЗПУО и във връзка с чл. 3, ал. 2 от Наредбата за минималните изисквания за мрежова и информационна сигурност (ДВ, БР. 59 от 19.07.2019 г.)

УТВЪРЖДАВАМ:

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

ДИРЕКТОР:

Татяна Петкова