ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ЗЕМЕДЕЛИЕ
“СТЕФАН ЦАНОВ” – ГР. К Н Е Ж А
общ.Кнежа, обл.Плевен, ул. “Марин Боев” №5, тел. 091327376, e-mail: info@pgzknezha.bg

УТВЪРЖДАВАМ:
ДИРЕКТОР: ИНЖ. СВЕТЛАНА КАЛАПИШЕВА

ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ЗЕМЕДЕЛИЕ „СТЕФАН ЦАНОВ” – ГР. КНЕЖА

ЗА УЧЕБНАТА 2022/2023 ГОДИНА

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1 Настоящата политика за мрежова и информационна сигурност определя ред, отговорности, способи и средства при осъществяване контрол и управление на работата на информационните системи в ПГЗ „Стефан Цанов“ - град Кнежа, както и дейностите, които трябва да се предприемат, за отговор на всякакъв вид инциденти, свързани със сигурността на информационните активи и отрицателно въздействие върху поверителността, целостта и наличността на информацията. 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.

Чл. 2 Документът касае и е приложим в работата на всички служители в институцията. Потребителите на информационни системи в ПГЗ „Стефан Цанов“ - град Кнежа са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 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 Наредба за минималните изисквания за мрежова и информационна сигурност.

РАЗДЕЛ II
КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 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

Чл. 5 Достъп до училищна Wi-Fi (безжична) мрежа в Професионална гимназия по земеделие “Стефан Цанов“ – гр. Кнежа през учебната 2022/2023 г., да имат педагогическия, непедагогическия персонал, ученици и гости.

Чл. 6 Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва от фирма „Димакс СОД“ ООД, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

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

Чл. 8 Лицата, които обработват лични данни, използват достатъчно сложни и уникални пароли, които не се записват или съхраняват онлайн. Индивидуалните пароли не се използват съвместно с други потребители.

Чл. 9 Всички пароли за достъп на системно ниво се променят периодично и при нужда.

Чл. 10 Всички носители на лични данни се съхраняват в безопасна и сигурна среда, с ограничен и контролиран достъп.

Чл. 11 На служителите на ПГЗ „Стефан Цанов“ - град Кнежа, които използват електронни бази данни и техни производни (текстове, разпечатки) се забранява:

(1) да ги изнасят под каквато и да е форма извън служебните помещения;

(2) да ги използват извън рамките на служебните си задължения;

(3) да ги предоставят на външни лица без да е заявена услуга.

Чл. 12 За нарушение целостта на данните се считат следните действия:

(1) унищожаване на бази данни или части от тях;

(2) повреждане на бази данни или части от тях;

(3) вписване на невярна информация в бази данни или части от тях.

Чл. 13 При изнасяне на носители извън физическите граници на ПГЗ „Стефан Цанов“ - град Кнежа, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 14 На служителите е строго забранено да използват мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него. Потребителите на мобилни компютърни средства и мобилни телефони отговарят за защитата им от кражба и не ги оставят без наблюдение.

Чл. 15 Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до зловреден софтуер. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл. 16 След като повече не са необходими, носителите 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.

Чл. 17 Събирането, подготовката и въвеждането на данни на интернет страницата се извършва от оправомощени служители на ПГЗ „Стефан Цанов“ - град Кнежа. Длъжностните лица притежават потребителски имена и пароли за актуализиране на сайта.

Чл. 18 Събирането и подготовката на данните се извършва от служителите, след което данните се предават в електронен вид (на файлове) на служителите отговорни за качването им на интернет страницата на общината.

РАЗДЕЛ III
РАБОТНО МЯСТО

Чл. 19 Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 20 Работното място се оборудва при спазване на изискванията на Наредба № 7 от 15.08.2005 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи (в сила от 25.11.2008 г.).

Чл. 21 Служителите да работят с предоставените им пароли за (Wi-Fi) мрежите PGZ-Teachers /учители/ и PGZ-Administration /администрация/ с повишено внимание и да ги опазват в тайна от трети лица /в това число ученици/.

Чл. 22 Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място или ползвани от него на сървъра на локалната компютърна мрежа съобразно дадените му права.

Чл. 23 Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола.

Чл. 24 Забранява се на външни лица работата с персоналните компютри на ПГЗ „Стефан Цанов“ - град Кнежа, освен за 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 Системния администратор.

Чл. 25 След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off.

Чл. 26 При загуба на данни или информация от служебния компютър, служителят незабавно уведомява прекия си ръководител и Системния администратор, който му оказва съответна техническа помощ.

Чл. 27 Забраняват се 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.

Чл. 28 Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на

комуникационни устройства се извършва само след съгласуване с фирма „Димакс СОД“ ООД.

Чл. 29 Забранява се използването на преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на ПГЗ „Стефан Цанов“ - град Кнежа.

Чл. 30 Служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

Чл. 31 Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи - идентификация на потребител, пароли, отчитане на времето на достъп, забрани за копиране, проследяване на неоторизиран достъп.

Чл. 32 Достъпът до помещенията, където са разположени комуникационните шкафове се ограничава по възможност само до фирма „Димакс СОД“ ООД.

Чл. 33 С оглед да се намали рискът от нерегламентиран достъп, загуба или повреждане на информацията в работно и извън работно време, се прилага политика на „чисти бюра“ и „чисти екрани“. Информацията, оставена на открито върху бюрата, също така може да бъде повредена или разрушена по време на бедствия, като например пожар, наводнение и др.

Процесът предвижда следните мерки за контрол:

• Където е уместно, хартиените и електронните носители се съхраняват в подходящи затворени шкафове и/или метални каси, когато не се използват и по-специално в извън работно време.

• Персоналните компютри и компютърни терминали и принтери не се оставят включени в системата, когато са оставени без наблюдение и са защитени посредством ключалки, пароли и други средства за контрол, когато не се използват.

• Местата с входяща и изходяща поща, които са оставени без наблюдение, са защитени с видеонаблюдение.

• Копирните машини се заключват и са защитени от нерегламентирано използване в извън работно време.

• Чувствителната или класифицирана информация, когато се отпечатва, се сваля от принтерите незабавно.

РАЗДЕЛ IV
ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 34 Фирма „Димакс СОД“ ООД извършва необходимите настройки за достъп до локалната мрежа (DC) и интернет като създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща на ПГЗ „Стефан Цанов“ - град Кнежа.

Чл. 35 Ползването на компютърната мрежа и електронна поща от служителите става чрез получените потребителско име и парола.

Чл. 36 Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.

Чл. 37 Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронна поща при използване на предоставените им потребителски имена и пароли.

Чл. 38 Компютрите, свързани в мрежата на училището използват интернет само от доставчик, с който ПГЗ „Стефан Цанов“ - град Кнежа има сключен договор за доставка на интернет.

Чл. 39 Забранява се свързването на компютри едновременно в мрежата на ПГЗ „Стефан Цанов“ - град Кнежа и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на ПГЗ „Стефан Цанов“ - град Кнежа и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и Наредба за минималните изисквания за мрежова и информационна сигурност.

Чл. 40 Забранява се инсталирането и използването на комуникатори (като ICQ, Skype, Viber, Facebook, Instagram, Snapchat, социални мрежи и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на ПГЗ „Стефан Цанов“ - град Кнежа 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 ПГЗ „Стефан Цанов“ - град Кнежа.

Чл. 41 Забранява се съхраняването на сървърите на ПГЗ „Стефан Цанов“ - град Кнежа на лични файлове с текст, изображения, видео и аудио.

Чл. 42 Забранява се отварянето без контрол от страна на фирма „Димакс СОД“ ООД:

(1) получени по електронна поща или на преносими носители изпълними файлове, файлове с мобилен код и файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg и архивни файлове;

(2) получени по електронна поща съобщения, които съдържат неразбираеми знаци.

РАЗДЕЛ V
ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 43 С цел антивирусна защита се прилагат следните мерки:

(1) Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.

(2) Фирма „Димакс СОД“ ООД извършва следните дейности:

2.1. активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;

2.2. настройва антивирусния софтуер за периодични сканирания през определен период, но поне веднъж седмично;

2.3. активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на системата;

2.4. проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер;

(3) При поява на съобщение от антивирусната програма за вирус в работна станция, всеки служител от съответното работно място задължително информира фирма „Димакс СОД“ ООД и прекия ръководител.

РАЗДЕЛ VI
НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 44 Следните мерки се прилагат с цел антивирусна защита:

1. Всички сървъри и устройства за съхранение на данни са свързани към устройства за непрекъсваемост на електрическо захранването.

2. При срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация. При възстановяване на мрежата, всички локално запазени файлове следва да се преместят отново на сървъра и да се изтрият локалните копия.

РАЗДЕЛ VII
СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 45 Осигурява се автоматизирано създаване на резервни копия на всички бази данни и електронни документи.

Чл. 46 Информацията, включително тази, съдържаща лични данни, се резервира по следния начин:

(1) Автоматизирано и планово се извършва архивиране на цялата работна информация дисковите масиви;

(2) Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг компютър и да се продължи работният процес без чувствителна загуба на данни;

РАЗДЕЛ VIII
УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Чл. 47 Изявяват се необходимите ресурси и се използват по организиран начин за противодействие на отрицателно въздействащи събития, свързани с надеждността и сигурността на информационните активи. Такива въздействия могат да са резултат от атаки, вируси и друг злонамерен код, опити за проникване и отказ от услуги, неразрешен достъп до или некоректно ползване на информационно-технологичните системи и данни и др.

Чл. 48 Дейности, свързани с работа по инцидентите:

(1) Пробивите в сигурността на информацията се докладват от всеки служител на директора на ПГЗ „Стефан Цанов“ - град Кнежа;

(2) Работата по инцидентите се извършва от фирма „Димакс СОД“ ООД;

(3) Инцидентите и предприетите действия се записват в протокол за посещение от фирма „Димакс СОД“ ООД;

(4) Отстраняване на последствията от инцидента възможно най-бързо.

РАЗДЕЛ IX
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в ПГЗ „Стефан Цанов“ - град Кнежа са длъжни да познават и спазват разпоредбите на тази Политика.

§ 2. Контролът по спазване на правилата се осъществява от Директора на училището.

§ 3. Настоящата политика се разглежда и оценява периодично с оглед ефективността й, като ПГЗ „Стефан Цанов“ - град Кнежа може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.