ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ТРАНСПОРТ "Н.Й.ВАПЦАРОВ"
гр.Сливница, ул."Кирил и Методий" №4, e-mail: : info-2300455@edu.mon.bg

ЗАПОВЕД
№71
29.09.2025 г.

На основание чл.259, ал.1 от ЗПУО и чл. 31, ал.1, т.2 от Наредба 15 от 22.07.2019 г. за статута и професионалното развитие на учителите, Закона за киберсигурност и Наредбата за минималните изисквания за мрежова и информационна сигурност, с цел осигуряване на безопасна и ефективна информационна среда в ПГТ "Н.Й.Вапцаров" - гр. Сливница,

У Т В Ъ Р Ж Д А В А М

Вътрешни правила за мрежова и информационна сигурност

за дейността на Професионалната гимназия по транспорт „Н.Й.Вапцаров" - гр. Сливница.

Директор:.....
Оля Зарева

Запознати:

Александър Георгиев.....

Мариана Григорова.....

УТВЪРЖДАВАМ:

Директор

Оля Зарева

ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ТРАНСПОРТ
"Н.Й.ВАПЦАРОВ"
гр.СЛИВНИЦА,ул."КИРИЛ И МЕТОДИЙ"№4,тел.0877963905
e-mail:info-2300455@edu.mon.bg, www.pgt-slivnitsa.bg

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

I. ОБЩИ ПОЛОЖЕНИЯ

1. Настоящите правила регламентират организацията и управлението на мрежовата и информационната сигурност в училището, в съответствие със Закона за киберсигурност и Наредбата за минималните изисквания за мрежова и информационна сигурност.
2. Основната цел е осигуряване на защита на данните, минимизиране на рисковете и ефективно противодействие на киберзаплахите.

II. ОРГАНИЗАЦИЯ НА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ

1. **Отговорности:**
   - Директорът на училището носи отговорност за общата политика по мрежова и информационна сигурност.
   - Назначава се администратор по сигурността на информационните и компютърни системи.
   - Всеки служител и ученик е длъжен да спазва правилата за сигурност при работа с мрежовите ресурси.
2. **Политики за достъп:**
   - Всеки потребител разполага с персонален акаунт за достъп до училищните системи и ресурси.
   - Препоръчителна е периодична смяна на паролите (на всеки 90 дни).
   - Препоръчително е използването на методи за двустепенно удостоверяване (2FA).
   - Ограничен достъп до административните и чувствителни данни само за оторизирани служители на училището.

III. ТЕХНИЧЕСКИ МЕРКИ ЗА ЗАЩИТА

1. **Мрежова сигурност:**
    - Използване на защитни стени (firewall) и антивирусен софтуер.
    - Ограничаване на достъпа до определени уебсайтове и приложения.
    - Редовно актуализиране на мрежовия и компютърен софтуер и хардуер.
2. **Физическа сигурност:**
    - Сървърните с мрежата на училището помещения се заключват и достъпът се контролира.
    - Забранява се свързването на неоторизирани устройства към училищната мрежа.
    - Свързването на устройства на гости на училището се случва само в определена за това мрежа от администратора по сигурността.
    - Използването на флашки, външни дискове и други преносими устройства е разрешено само със служебно одобрение.
    - Преносимите носители задължително се сканират за вируси преди използване в училищната мрежа.
    - Забранява се копирането на чувствителни данни от училищните компютри на лични устройства.
    - Учениците нямат право да свързват лични USB устройства към училищните компютри без разрешение от администратора по сигурността на училището.

IV. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

1. Всеки инцидент, свързан със сигурността на информацията, се докладва на администратора по сигурността и директора на училището.
2. В случай на кибератака се предприемат незабавни мерки по изолиране на засегнатите системи от администратора по сигурността.
3. Води се регистър на инцидентите и анализ за предотвратяване на бъдещи пробиви.

V. ОБУЧЕНИЕ И КОНТРОЛ

1. Периодично обучение на персонала и учениците за киберрисковете и добрите практики.
2. Провеждане на вътрешноинституционални обучения и оценка на персонала.

VI. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Настоящите правила влизат в сила от датата на утвърждаването им от директора на училището.
2. Всички служители и ученици са длъжни да се запознаят с тях и да ги спазват.