



ЦЕНТЪР ЗА СПЕЦИАЛНА ОБРАЗОВАТЕЛНА ПОДКРЕПА  
„ПРОФ. ДПН ГЕОРГИ АНГУШЕВ”  
СОФИЯ, РАЙОН ИЛИНДЕН, БУЛ. „ТОДОР АЛЕКСАНДРОВ” №175  
Тел.: 0878 924 661; e-mail: [info-2206613@edu.mon.bg](mailto:info-2206613@edu.mon.bg)



Утвърдил: .....

Директор: Александра Миленкова

## ВЪТРЕШНИ ПРАВИЛА

по мрежова и информационна сигурност

на ЦСОП „Проф. дпн Георги Ангушев“

Настоящите вътрешни правила са задължителни за всички служители на ЦСОП „Проф. дпн Георги Ангушев“. Тяхната цел е да установят единни процедури в съответствие с националното законодателство, стандарта ISO/IEC 27001 и политиките на Столична община, гарантирайки защита на данните на учениците, персонала и информационните активи на центъра.

### 1. Класифициране на документираната информация

Всички данни и документи, създадени в рамките на трудовия процес, са собственост на ЦСОП „Проф. дпн Георги Ангушев. Използва се четиристепенна система TLP (Traffic Light Protocol):

| Ниво              | Етикетиране                                                  | Обмен                                      | Съхранение                    | Унищожаване    |
|-------------------|--------------------------------------------------------------|--------------------------------------------|-------------------------------|----------------|
| Ниво 0<br>(WHITE) | Не е нужно                                                   | Публично свободно                          | Стандартни<br>правила         | Без изисквания |
| Ниво 1<br>(GREEN) | При споделяне<br>извън ЦСОП<br>„Проф. дпн Георги<br>Ангушев“ | Ограничен кръг<br>заинтересовани<br>страни | Свободно в<br>рамките на ЦСОП | Без изисквания |

| Ниво              | Етикетиране                                          | Обмен                                                                             | Съхранение                                             | Унищожаване                                             |
|-------------------|------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------|---------------------------------------------------------|
| Ниво 2<br>(AMBER) | Задължително.<br>Горен десен ъгъл,<br>Bold, Size 12+ | Само между<br>оторизирани лица;<br>криптиран е-майл;<br>лично предаване в<br>плик | Заклучени<br>шкафове;<br>криптирани<br>дигитални папки | Шредер (хартия);<br>физическо унищожаване<br>(носители) |
| Ниво 3<br>(RED)   | Критично.<br>Обозначение на<br>всяка страница        | Само лично на ръка<br>или чрез TLS 1.2+<br>криптиране (мин.<br>256 бита)          | Каса/Сейф; КЕП<br>идентификация за<br>цифрови данни    | Шредер;<br>изгаряне/натрошаване на<br>носители          |

## 2. Мобилни устройства и преносими носители

- **Лични устройства (BYOD):** Използването на лични телефони/лаптопи за служебни цели (достъп до дневници, досиета) се допуска само след одобрение от системния администратор/директора.
- **Защита:** Всички устройства трябва да имат PIN (мин. 4 знака) или биометрия.
- **Пренос:** Лаптопите се пренасят само в защитни чанти. При загуба се докладва незабавно.
- **Външни носители:** Използването на лични USB памети в служебната мрежа е **забранено**. Служебните USB трябва да бъдат криптирани при пренос на чувствителни данни (Ниво 2 и 3).

## 3. Работа от разстояние и облачни услуги

- **Мрежова сигурност:** Забранява се използването на обществени Wi-Fi мрежи (кафенета, гари) за достъп до административни системи. Препоръчва се използването на мобилни данни (Hotspot) или VPN.
- **Контрол:** Екраните се заключват винаги, когато служителят не е пред тях. Достъпът на членове на семейството до служебни устройства е недопустим.

## 4. Пароли и автентификация

- **Сложност:** Минимум 8 символа (главни/малки букви, цифри, знаци).

- **Забрани:** Забранено е записването на пароли на листчета („post-it“ бележки) по монитори или под клавиатури.
- **Споделяне:** Паролите са строго индивидуални. Споделянето им с колеги е дисциплинарно нарушение.

## 5. „Чисто бюро и чист екран“

- В края на работния ден или при напускане на кабинета, всички документи с чувствителна информация (планове за подкрепа, медицински документи) трябва да са прибрани в заключващи се шкафове.
- Компютрите се заключват с комбинация **Win + L**.
- Забравени документи в принтера/копирната машина се считат за риск за сигурността.

## 6. Инсталиране на софтуер и интернет ползване

- Инсталирането на софтуер се извършва само от оторизиран техник.
- **Електронна поща:** Служебният имейл не се ползва за лични регистрации (пазаруване, игри).
- **Внимание:** При получаване на съмнителен имейл („фишинг“), прикаченият файл не се отваря и се уведомява системният администратор.

## 7. Изкуствен интелект (ИИ)

- Използването на инструменти като ChatGPT за обработка на текстове е позволено, **НО** е строго забранено въвеждането на:
  - Имена и лични данни на ученици/родители.
  - Информация от ниво **AMBER** и **RED**.
- Служителят носи пълна отговорност за фактологическата точност на генерираното от ИИ съдържание.

## 8. Докладване на инциденти

Всеки служител е длъжен да докладва на Директора или Системния администратор при:

- Съмнение за вирус или хакерска атака.
- Загуба на служебна карта, ключ или устройство.
- Случайно разкриване на лични данни на трети лица.

## **9. Дисциплинарна отговорност**

Нарушаването на тези правила се счита за нарушение на трудовата дисциплина. При установен пробив в сигурността, Директорът на ЦСОП назначава комисия за разследване, която може да предложи налагане на дисциплинарни наказания съгласно КТ.

**Дата:** 21.03. 2026 г.