



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



Утвърдил:

Директор: Александра Миленкова

ПОЛИТИКА ПО КИБЕРСИГУРНОСТ

НА ЦСОП „ПРОФ. ДПН ГЕОРГИ АНГУШЕВ“

Настоящата политика е разработена съобразно Закона за киберсигурност (ЗКС), Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС) и специфичните изисквания за защита на данните в системата на предучилищното и училищното образование.

1. ОБХВАТ И ПРИЛОЖИМОСТ

Политиката обхваща всички аспекти на дейността на ЦСОП „Проф. дпн Георги Ангусhev“. Тя е задължителна за:

- Педагогическия и непедагогическия персонал;
- Външни специалисти и терапевти, работещи с центъра;
- Информационните системи (НЕИСПУО, дневници, счетоводен софтуер);
- Всички крайни устройства (компютри в кабинети, таблети за терапия, сървъри).

2. ОСНОВНИ ПРИНЦИПИ И ЦЕЛИ

2.1. Принципи: Поверителност (защита на досиетата на учениците), Целост (точност на терапевтичните оценки), Наличност (достъп до образователни ресурси), Отчетност и Неотричане.

2.2. Цели:

1. Защита на чувствителната информация за здравословното и психологическо състояние на учениците.

2. Осигуряване на непрекъснатост на образователния и терапевтичен процес.
3. Минимизиране на рисковете от загуба на данни при работа с облачни платформи.

3. ОРГАНИЗАЦИОННА СТРУКТУРА И ОТГОВОРНОСТИ

3.1. Ръководство: Директорът на ЦСОП „Проф. д-н Георги Ангушев“ носи крайната отговорност за киберсигурността и осигурява ресурси за ИТ поддръжка.

3.2. Отговорно лице (ОЛМИС): Директорът определя служител или външен експерт (системна администрация), който координира мерките за сигурност, актуализира софтуера и е точка за контакт при инциденти.

3.3. Служители: Учители, терапевти и администрация са длъжни да използват системите отговорно, да не споделят пароли и да докладват незабавно за „странно“ поведение на компютрите.

4. УПРАВЛЕНИЕ НА РИСКА

„Проф. д-н Георги Ангушев“ извършва годишна оценка на риска, като се фокусира върху:

- Риск от изтичане на лични данни на ученици (Ниво: Високо).
- Риск от прекъсване на работата на административните системи (Ниво: Средно).
- Заплахи от фишинг атаки към служителите (Ниво: Средно).

5. УПРАВЛЕНИЕ НА ДОСТЪПА

- **Минимални привилегии:** Учителите имат достъп само до данните на учениците, с които работят. Административният персонал няма достъп до терапевтичните картони, освен ако не е необходимо.
- **Автентикация:** Използване на уникални акаунти. Забранено е ползването на общ акаунт „Teacher“ или „Cabinet“.
- **Автоматично заключване:** Екраните в кабинетите за терапия се заключват автоматично след 5 минути неактивност, за да се предотврати достъп на външни лица или ученици до системата.

6. ЗАЩИТА ОТ ЗЛОВРЕДЕН СОФТУЕР И ОБНОВЯВАНЕ

- **Антивирус:** Всички компютри и таблети за работа с деца трябва да имат активна и обновена защита.
- **Актуализации:** Операционните системи се обновяват автоматично извън часовете за терапия.
- **Забрана:** Служителите нямат право да инсталират игри или нелицензиран софтуер на служебните устройства.

7. СИГУРНОСТ НА КОМУНИКАЦИИТЕ

- **Електронна поща:** Официалната комуникация с родители и институции се води само през служебни имейли.
- **Wi-Fi:**

В ЦСОП „Проф. д-н Георги Ангусев“ се поддържат две отделни мрежи:

1. **Служебна (Администрация):** Скрита, със силно криптиране.
2. **Образователна (Ученици/Гости):** Изолирана от административните данни.

8. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

При съмнение за пробив (изчезнали файлове, заключен екран с искане за откуп, съмнителен имейл):

1. Служителят изключва устройството от мрежата (изважда кабела или спира Wi-Fi).
2. Докладва незабавно на ОЛМИС/Директора.
3. ОЛМИС анализира инцидента и при нужда уведомява националния екип за реагиране (CERT).

9. НЕПРЕКЪСНАТОСТ И РЕЗЕРВНИ КОПИЯ

- **Back-up:** Веднъж седмично се прави резервно копие на счетоводната база и базата с данни на учениците на защитен външен носител или криптиран облак.
- **План при срив:** При техническа авария административните процеси преминават временно на хартиен носител до възстановяване на системите.

10. ФИЗИЧЕСКА СИГУРНОСТ

- Сървърното оборудване и комуникационните шкафове се намират в заключени помещения/шкафове с ограничен достъп.
- Критичните устройства са подсиgurени с UPS (непрекъсваемо захранване).

11. ОБУЧЕНИЕ

Всеки нов служител преминава инструктаж по киберсигурност в рамките на първата работна седмица. Провеждат се ежегодни кратки обучения за разпознаване на фишинг и сигурна работа в мрежата.

Дата: 21.03. 2026 г.