ОСНОВНО УЧИЛИЩЕ „ГЕОРГИ СТОЙКОВ РАКОВСКИ”
с. ГЪЛЪБЕЦ общ. ПОМОРИЕ обл. БУРГАС ул. „Пирин” № 32
Директор 0884132969 E-mail:200707@edu.mon.bg

ПРОЦЕДУРА ЗА ДЕЙСТВИЕ ПРИ НАРУШАВАНЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ В ОСНОВНО УЧИЛИЩЕ „ГЕОРГИ СТОЙКОВ РАКОВСКИ“ С.ГЪЛЪБЕЦ

1. Цел и обхват
Тази процедура установява стъпките, които служителите на училището трябва да предприемат в случай на потенциално или действително нарушение на сигурността (загуба, кражба, неправомерен достъп или случайно унищожаване на данни).

2. Какво се счита за "Нарушение"?
- **Загуба или кражба** на лаптоп, USB памет или хартиени досиета.
- **Хакерска атака** или заразяване на училищната мрежа с вирус/ransomware.
- **Грешка при изпращане:** Имейл с чувствителна информация (напр. оценки, здравен статус), изпратен до грешен родител или публикуван публично.
- **Неоторизиран достъп:** Служител или външно лице разглежда данни, за които няма правомощия.

3. План за действие (Стъпка по стъпка)

Стъпка 1: Вътрешно докладване (Незабавно)
Всеки служител, който установи проблем, е длъжен да докладва на **Длъжностното лице по защита на данните (DPO)** или на **Директора** в рамките на **1 час** от установяването.
- *Не се опитвайте да поправяте проблема сами, преди да сте го документирали.*

Стъпка 2: Сформиране на екип и анализ
Директорът и DPO оценяват:
- Какъв е обемът на засегнатите данни?
- Има ли риск за правата и свободите на учениците/родителите (напр. риск от кражба на самоличност, дискриминация, психологически стрес)?

Стъпка 3: Овладяване на риска
- Изолиране на компрометираните системи (изключване на сървъри, смяна на пароли).
- Опит за възстановяване на архиви (backups).
- Ако е възможно – дистанционно изтриване на данни от откраднатото устройство.

Стъпка 4: Уведомяване на КЗЛД (до 72 часа)
Ако нарушението представлява риск за лицата, училището е длъжно да уведоми **Комисията за защита на личните данни (КЗЛД)** в рамките на 72 часа.
Уведомлението съдържа:
1. Естество на нарушението.
2. Приблизителен брой засегнати лица.
3. Евентуални последици.
4. Предприети мерки.

Стъпка 5: Уведомяване на засегнатите лица (родители/ученици)
Ако има **висок риск** (например изтичане на ЕГН, пароли или медицински картони), училището трябва незабавно да информира родителите на засегнатите деца, като им даде съвети как да се предпазят.

4. Регистър на нарушенията
Всяко нарушение, независимо дали е докладвано на КЗЛД или не, се вписва в специален **Вътрешен регистър на нарушенията**, който включва:

- Факти около инцидента.
- Последици.
- Действия по отстраняване.

5. Превантивни мерки

- Редовно обучение на учителите за разпознаване на фишинг атаки.
- Използване на криптирани USB устройства.
- Задължително заключване на кабинети и шкафове с досиета.

Тази процедура е утвърдена със заповед на Директора №235/28.05.20218 г. и с нея са запознати всички служители срещу подпис.