

ДГ“ ПИКАЗЕН СВЯТ“, С. МАЙСКО, УЛ. ПЪРВА №61, E- mail:info-310314@edu.mon.bg

МЕРКИ ЗА УПРАВЛЕНИЕ НА РИСКА И ЗАДЪЛЖЕНИЯ ЗА ДОКЛАДВАНЕ В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА

НА

ДЕТСКА ГРАДИНА „ПРИКАЗЕН СВЯТ“

Версия: 1.0

2026 г.

Съдържание:

1. ОБХВАТ И ЦЕЛ.....	1
2. МЕРКИ ЗА УПРАВЛЕНИЕ НА РИСКА	1
3. ОТГОВОРНОСТИ.....	5
4. МОНИТОРИНГ И ПРЕГЛЕД	3
5. ЗАДЪЛЖЕНИЯ ЗА ДОКЛАДВАНЕ	4

1. ОБХВАТ И ЦЕЛ

Обхват:

Този документ определя мерките за управление на риска и задълженията за докладване на образователната институция съгласно Закона за киберсигурност (ЗК) включително и последни изменения от 2026 г.

Цел:

- Да се осигури високо ниво на киберсигурност чрез прилагане на адекватни и пропорционални мерки.
- Да се гарантира своевременното докладване на киберинциденти, съгласно законовите изисквания.
- Да се улесни изпълнението на задълженията за докладване към компетентните органи.

2. МЕРКИ ЗА УПРАВЛЕНИЕ НА РИСКА

Мерките следват изискванията на ЗК и са групирани в четири основни направления:

2.1. Технически мерки

- **Контрол на достъпа:** Строги правила за удостоверяване (MFA/2FA), управление на

Примерни мерки за управление на риска и задължения за докладване в областта на киберсигурността

привилегировани акаунти (PAM), принцип на „най-малко привилегии“.

- **Мрежова сегментация:** Изолиране на критичните системи от публичната мрежа и взаимно между отделните сегменти.
- **Шифроване:** Шифроване на данни в покой и при пренос, използвайки утвърдени алгоритми и ключова инфраструктура (HSM).
- **Защита на крайни точки:** Антивирусни решения, EDR, XDR и централизирано управление на пачовете.
- **Системи за откриване и предотвратяване:** IDS/IPS, SIEM, SOAR, WAF, DDoS защита.
- **Управление на уязвимости:** Редовни сканирания за уязвимости и незабавно прилагане на пачове/работни заобикаляния.
- **Архивиране и възстановяване:** Редовно архивиране на критични данни и планове за възстановяване при бедствия (Disaster Recovery Plan – DRP), включително офсайт/облачни копия.
- **Сигурност на доставчиците:** Задължителни клаузи за киберсигурност в договорите с трети страни.

2.2. Организационни мерки

- **Политики и процедури:** Въвеждане на политики за управление на риска, инциденти, непрекъсваемост на бизнеса и сигурност на доставчиците.
- **Управление на идентичности и достъп (IAM):** Централизирано управление на потребителските акаунти, ролево базиран достъп.
- **Управление на промените:** Строго контролирани и документирани процеси за внедряване на нови технологии и софтуер.
- **Обучение на персонала:** Редовни обучения по киберсигурност (вкл. фишинг симулации) за всички служители.
- **Планове за реагиране при инциденти (IRP):** Разработени, тествани и актуализирани планове за реакция при киберинциденти, включително комуникационни протоколи.
- **Тестове и проверки:** Провеждане на penetration testing, vulnerability assessments, red teaming и други.

2.3. Правни и регулаторни мерки

- **Съответствие със законодателството:** Пълно съответствие със ЗК, GDPR, секторни закони и европейското право.
- **Договорни клаузи:** Включване на задължителни киберсигурност клаузи в

Примерни мерки за управление на риска и задължения за докладване в областта на киберсигурността

договорите с доставчици и клиенти.

- **Лицензионни и разрешителни изисквания:** Спазване на всички лицензионни и разрешителни режими, свързани с дейността.

2.4. Управление на доставчиците (Third-Party Risk Management)

- **Оценка на доставчиците:** Предварителна оценка на нивото на киберсигурност на доставчиците (чрез въпросници, одити, сертификати).
- **Договорни задължения:** Включване на специфични клаузи за отчетност при инциденти, право на одит и спазване на същите стандарти за сигурност.
- **Мониторинг и преглед:** Периодичен мониторинг и повторни оценки на доставчиците.

3. ОТГОВОРНОСТИ

Роля	Отговорност
Ръководител на образователната институция	Отговаря за утвърждаването на мерките и осигуряване на възможност за тяхното прилагане
Отговорник „Киберсигурност“/Отговорник СУСИ	Носи крайната отговорност за внедряване и поддържане на мерките за управление на риска и за осигуряване на спазване на задълженията за докладване. Отговаря за първоначалното разследване на инцидентите, уведомяването на СЕРИКС и подготовката на окончателния доклад.
Системен администратор/ИТ експерт	Отговаря за прилагането на техническите мерки и поддръжката на системите.
Ръководители / заместник-директори и други	Отговарят за оценката и мониторинга на доставчиците. Отговарят за прилагането на организационните мерки и обучението на персонала.

4. МОНИТОРИНГ И ПРЕГЛЕД

- Мерките за управление на риска се преглеждат **най-малко веднъж годишно** или при значителни промени в средата, процесите или законодателството.

Примерни мерки за управление на риска и задължения за докладване в областта на киберсигурността

- Ефективността на мерките се оценява чрез вътрешни одити, penetration tests, vulnerability scans и анализ на инциденти.
- Резултатите от оценката се докладват на Съвета на директорите и НКЦК при поискване.

5. ЗАДЪЛЖЕНИЯ ЗА ДОКЛАДВАНЕ

Задълженията за докладване на киберинцидент са регламентирани в ЗКС:

Киберинцидент: значителен инцидент

Ранно предупреждение: Образователната институция уведомят СЕРИКС в което, когато е приложимо, се посочва дали се предполага, че значителният инцидент се дължи на незаконосъобразни или злонамерени действия и дали би могъл да има трансгранично въздействие – **не по-късно от 24 часа** от установяването му.

Уведомление за инцидент: до 72 часа след установяването на значителния инцидент, в което, когато е приложимо, се актуализира информацията и се посочва първоначална оценка на значителния инцидент, включително неговата тежест и въздействие, както и, когато има такава, техническа информация за инцидента

Междинни доклади: При необходимост се подават междинни доклади за развитието на инцидента и предприетите действия.

Окончателен доклад: Не по-късно от един месец след подаването на уведомлението за инцидента по т. 2, включващ:

- а) подробно описание на инцидента, включително неговите обхват и въздействие;
- б) вида на заплахата или причината, която вероятно е породила инцидента;
- в) приложените и текущите мерки за ограничаване на инцидента;
- г) когато е приложимо, трансграничното въздействие на инцидента;