



МАТЕМАТИЧЕСКА ГИМНАЗИЯ “ГЕО МИЛЕВ” – ПЛЕВЕН

5800 Плевен, ж.к. “Сторгозия”, директор: 064 680 996, тел. канцелария: 064 680 802

Утвърдил:

 Recoverable Signature

X Диана Данова

Signed by: DIANA MILKOVA DANOVA

ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата Политика за мрежова и информационна сигурност (МИС) е разработена в съответствие със Закона за киберсигурност (ЗКС) (обн. ДВ. бр. 94 от 2018 г., с изм. и доп. ДВ. бр. 17 от 13 февруари 2026 г., транспониращ Директива (ЕС) 2022/2555 – NIS 2), Наредбата за минималните изисквания за мрежова и информационна сигурност и действащото законодателство в областта на защита на личните данни (GDPR) и има за цел осигуряването на контрол и управление на работата на информационните системи в МГ „Гео Милев“ – Плевен. В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, включително видеонаблюдение, програмни продукти, данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми.

Чл. 2. Потребителите на информационни системи в МГ „Гео Милев“ - Плевен са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3. Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Наредбата за минималните изисквания за мрежова сигурност.

РАЗДЕЛ II. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 4. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

1. **Разделяне на първоначални потребителски от администраторски функции.**
2. Установяване на нива на достъп до информация.
3. Регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация.
4. Техниката да се използва за служебни цели.
5. Не се позволява инсталирането на какъвто и да е нов и реконфигурирането от потребителите на вече инсталиран софтуер и хардуер, както и самостоятелни

опити за поправка или подобрения на горепосочените. При съмнение за възникнал проблем незабавно се уведомява ръководителя на направление „ИКТ“.

6. Не се позволява използването на внесени отвън софтуер и хардуер.
7. Използването на внесени отвън информационни носители (оптични дискове, флаш памет и др.) става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, носителите не се използват.
8. Не се допускат външни лица до комуникационните шкафове и техниката за интернет- връзка, с изключение на техници от оторизирани фирми и то само придружени от ръководителя на направление „ИКТ“.
9. Не се допуска достъпа на външни лица до компютърната техника в административните помещения в сградата на МГ „Гео Милев“ - Плевен.
10. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.
11. Паролите за достъп на всички ученици и служители се раздават от ръководителя на направление „ИКТ“. Всички пароли за достъп на системно ниво се променят периодично от служителите.

Чл. 5. (1) Училището управлява рисковете, произтичащи от отношенията му с външни доставчици на продукти, услуги и цифрови платформи (в т.ч. доставчици на електронни дневници, облачни услуги, хостинг, софтуерни лицензи и ИТ поддръжка). (2) Преди сключване или подновяване на договори с външни изпълнители, Директорът извършва оценка на киберсигурността на доставчика, като изисква доказателства за внедрени стандарти за сигурност. (3) Всички нови договори с доставчици на ИТ услуги задължително включват клаузи за конфиденциалност, ангажимент за незабавно уведомяване при пробив в техните системи и съответствие с изискванията на ЗКС.

Чл. 6. (1) Достъпът на педагогическия и административния персонал до критични училищни ресурси и информационни масиви (включително облачни платформи, служебни електронни пощи и административни панели) се осъществява задължително чрез многофакторна автентикация (MFA). (2) Вписването и обработката на лични данни на ученици и персонал да се извършва от защитени устройства. (3) Училището поддържа актуален План за непрекъсваемост на дейността, който включва ежедневни автоматизирани резервни копия (back-up) на критичните данни, съхранявани в изолирана среда, с цел бързо възстановяване на учебния процес при кибератака (напр. Ransomware).

Чл. 7. Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили.

Чл. 8. Предоставянето на достъп става чрез заповед, като се задават определени права на

достъп до конкретни информационни ресурси, според заемната длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

Чл. 9. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн.

Чл. 10. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 11. Всички носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп.

Чл. 12. На служителите на МГ „Гео Милев“ - Плевен, които използват електронни бази данни и техни производни се забранява:

- да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга);
- да ги използват извън рамките на служебните си задължения;
- да ги предоставят на външни лица без да е заявена услуга.

Чл. 13. За нарушение целостта на данните се считат следните действия:

- унищожаване на бази данни или части от тях;
- повреждане на бази данни или части от тях;
- вписване на невярна информация в бази данни или части от тях.

Чл. 14. При изнасяне на носители извън физическите граници на МГ „Гео Милев“ - Плевен, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 15. На служителите е строго забранено да използват служебни мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него.

Чл. 16. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл. 17. След като повече не са необходими, носителите се унищожават сигурно и безопасно за намаляване на риска от изтичане на чувствителна информация към неупълномощени лица. Физическото унищожаване на информационните носители става със счупване. Предварително се проверят, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

РАЗДЕЛ III. РАБОТНО МЯСТО

Чл. 18. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 19. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място.

Чл. 20. Служителят има право да работи на служебен компютър, като достъпът до

съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола.

Чл. 21. Забранява се на външни лица работата с персоналните компютри на МГ „Гео Милев“ - Плевен, освен за:

- упълномощени фирмени специалисти в случаите на първоначална инсталация на компютърна и периферна техника, програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствие на директор, заместник-директор или ръководителя на направление „ИКТ“;
- провеждане на олимпиади и състезания при задължително присъствие на ръководителя на направление „ИКТ“.

Чл. 22. След края на работния ден всеки служител задължително изключва компютъра, на който работи.

Чл. 23. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява ръководителя на направление „ИКТ“, който му оказва съответна техническа помощ.

Чл. 24. Забраняват се опити за достъп до компютърна информация и бази данни, до които не са предоставени права, съобразно заеманата от служителя длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп.

Чл. 25. Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства се извършва само след съгласуване с ръководителя на направление „ИКТ“.

Чл. 26. Забранява се използването на преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на МГ „Гео Милев“ - Плевен.

Чл. 27. Служителите имат право да обменят компютърна информация само във връзка с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

Чл. 28. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача.

Чл. 29. Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи - идентификация на потребител, пароли, отчитане на времето на достъп, забрани за копиране, проследяване на несанкциониран достъп.

Чл. 30. Достъпът до помещенията с комуникационните шкафове се ограничава.

РАЗДЕЛ IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 31. Компютрите, свързани в мрежата на МГ „Гео Милев“ - Плевен, използват интернет само от доставчик, с когото училището има сключен договор за доставка на интернет.

Чл. 32. Фирмата, доставчици на интернет услуги и ремонт не променят изградената вътрешна мрежа с необходимите мрежови комутатори, рутери, защитни стени; избира техническите устройства, извършва необходимите настройки за достъп до интернет, разделя логически локалната мрежа на четири отделни мрежи – локална мрежа за администрация, локална мрежа за учители, локална мрежа за ученици и локална мрежа за гости и създава потребителски имена и пароли за работа с компютърната мрежа.

Чл. 33. Ползването на компютърната мрежа и електронните платформи от служителите става чрез получените потребителско име и парола.

Чл. 34. Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.

Чл. 35. Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронните платформи при използване на предоставените им потребителски имена и пароли.

Чл. 36. Забранява се съхраняването на компютрите на МГ „Гео Милев“ - Плевен на лични файлове с текст, изображения, видео и аудио.

Чл. 37. Забранява се отварянето без контрол от страна на системния администратор на:

- получени по електронна поща или на преносими носители изпълними файлове, файлове с мобилен код и файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg и архивни файлове;
- получени по електронна поща съобщения, които съдържат неразбираеми знаци.

Чл. 38. Не се толерира влизането в Интернет - сайтове с неизвестно съдържание.

РАЗДЕЛ V. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 39. С цел антивирусна защита се прилагат следните мерки:

- Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява.
- Ръководителят на направление „ИКТ“ и учителите по информатика и ИТ извършват следните дейности:

- активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;
- настройва антивирусния софтуер за периодични сканирания през определен период;
- активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на системата;
- проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер.

Чл. 40. При липса на ел. захранване за повече от 10 минути, служителите са длъжни да започнат процедура за спиране на устройствата за съхранение на данни.

Чл. 41. Всеки служител, който работи с класифицирана информация, осигурява автоматично създаване на архивни копия периодично.

Чл. 42. Информацията, включително тази, съдържаща лични данни, се резервира по следните начини:

1. Автоматизирано и планово се извършва архивиране на цялата работна информация на запаметяващите устройства и дисковите масиви.
2. Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг компютър и да се продължи работният процес без чувствителна загуба на данни.
3. Базите данни от програми в счетоводството се архивират всеки ден в края на работното време:

РАЗДЕЛ VII ВИДЕОНАБЛЮДЕНИЕ

Чл. 43. (1) Реда и условията за осъществяване на видеонаблюдение на територията на МГ „Гео Милев“ – гр. Плевен, както и правата на физическите лица, чиито лични данни се събират и обработват чрез него се извършва по общите правила в случаите на събиране на лични данни чрез видеонаблюдение.

(2) Данните от видеозаписите са лични данни по смисъла на Общия регламент за защита на личните данни, като МГ „Гео Милев“ се явява Администратор на лични данни, а физическите лица – субекти на лични данни.

Чл. 44. (1) Видеонаблюдението се осъществява във фойетата и коридорите, учебните стаи и двора на училището.

- (2) Видеосистемата се поддържа от фирма, с която училището има сключен договор.
- (3) Видеонаблюдението се осъществява от 42 вътрешни камери (25 в стаи и 17 в коридори) и 6 външни камери
- (4) Видеозаписващите устройства и монитори за наблюдение към тях се намират в кабинета на директор.

Чл. 45. (1) Училището използва системата за видеонаблюдение за следните цели:

1. Осигуряване на безопасност и сигурност;
2. Защита на живота и здравето на учениците, персонала и посетителите в сградата;
3. Превенция и разкриване на нарушения.
4. Опазване на материалната база

(2) При необходимост видеонаблюдението допълва други системи за физическа сигурност, като:

1. Система за контрол на достъпа;
2. Система за контрол срещу физическо проникване.

(3) Системата за видеонаблюдение **не се използва** за:

1. Наблюдение на работата на персонала;
2. Проследяване на присъствието на служители или ученици.

(4) В изключителни случаи видеонаблюдението може да се използва за:

1. Разследване на инциденти, свързани с физическата сигурност;
2. Подпомагане на наказателни разследвания, при необходимост и в съответствие

с действащото законодателство.

Чл. 46. (1) Достъп до данните от видеонаблюдението имат:

1. Директорът на гимназията или упълномощено от него лице;
2. Лицата, определени със заповед за обработващи лични данни;
3. Представители на държавни органи (МВР, съд, прокуратура и др.), при надлежно

представени документи.

(2) Всяко лице, обект на видеонаблюдение, има право на достъп до собствените си лични данни в съответствие с Регламент (ЕС) 2016/679 (GDPR) и Закона за защита на личните данни (ЗЗЛД).

(3) Исканията за достъп се подават в писмена форма по утвърден образец до директора на училището. (Приложение 2 и Приложение 3)

Чл. 47. Когато искането за достъп до видеозапис засяга и други ученици/деца или служители, достъпът се осигурява при спазване на следните условия:

1. Да се поиска и получи изрично писмено съгласие от родителите на всички останали ученици/деца и/или други засегнати субекти, заснети и идентифицируеми от записа. В този случай може да се предостави копие от видеозаписа на заявителя.
2. Да се предоставят стопкадри (screenshots), на които се вижда само детето/лицето на заявителя, а образите на третите лица са заличени.
3. Да се осигури достъп чрез преглед на място на видеозаписа, само при условие че родителите/засегнатите лица на всички други засегнати ученици/деца и/или служители присъстват едновременно и подписват декларация, че:
 - 3.1. Се съгласяват да се извърши преглед на записа (на конкретна дата и в присъствието на всички засегнати субекти);

3.2. Няма да разгласяват или разпространяват информацията;
4. При този преглед не е допустимо да се извършва презапис с лични или други устройства.

Чл. 48. Субектите на данни имат право:

1. Да получат информация за целите, обхвата и начина на видеонаблюдение;
2. Да поискат достъп до записи, в които фигурират;
3. Да поискат коригиране или ограничаване на обработването на данните, когато това е приложимо;
4. Да подадат жалба до Комисията за защита на личните данни (КЗЛД).

Чл. 49. Отговорности и срокове на съхранение на видеозаписите (Приложение 1)

(1) Записите от видеонаблюдението се съхраняват за срок до 15 календарни дни, освен ако не са необходими за целите на образувано разследване или производство.

(2) След изтичане на срока записите се унищожават автоматично по начин, недопускащ възстановяване.

Чл. 50. На всички входи на училището и в зоните с видеонаблюдение се поставят ясни и видими информационни табели, съдържащи уведомление, че се осъществява видеонаблюдение;

РАЗДЕЛ VIII. ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ В ОБУЧЕНИЕТО

Чл. 51. Използването на инструменти с Изкуствен интелект (ИИ) в административната и учебната дейност на училището се допуска само с образователна цел и при спазване на правилата за защита на личните данни.

Чл. 52. При работа с публични платформи (като ChatGPT, Gemini и др.) НЕ се допуска споделянето на конфиденциална училищна информация, вътрешни документи, бюджети, както и лични данни на ученици и персонал.

Чл. 53. Учениците и служителите нямат право да използват ИИ за създаване на дълбоки фалшификати (deepfakes), генериране на обидно, дискриминационно или подвеждащо съдържание в рамките на училищната мрежа и устройства.

Чл. 54. Всеки пробив в сигурността или установен опит за измама чрез използване на ИИ се докладва незабавно на Отговорника по мрежова и информационна сигурност в училището.

РАЗДЕЛ IX. ОТГОВОРНОСТ, УПРАВЛЕНИЕ И УВЕДОМЯВАНЕ ПРИ КИБЕРИНЦИДЕНТИ

Чл. 55. Директорът на училището, в качеството си на управителен орган, носи пряка лична отговорност за одобряването, прилагането и контрола на мерките за управление на рисковете за киберсигурността в институцията.

Чл. 56. (1) Директор и Заместник-директори, ръководителя на направление „ИКТ“ са длъжни да преминават специализирано обучение за придобиване на достатъчно знания и умения за идентифициране на рисковете и оценка на практиките за управление на киберсигурността.

(2) Обучението по ал. 2 се провежда периодично, **най-малко веднъж на всеки 2 (две) години**, като документираните сертификати или протоколи се съхраняват в досието на институцията.

Чл. 57. (1) Всички служители са длъжни незабавно да докладват на Директора или ръководителя на направление „ИКТ“ за всяко събитие, което компрометира или има потенциал да компрометира сигурността на училищната мрежа, електронните дневници, базите данни или официалния сайт.

(2) При възникване на значителен инцидент, Директорът организира двуетапно уведомяване на Националния екип за реагиране на инциденти с компютърната сигурност (CERT) към Министерството на електронното управление в следните задължителни срокове:

1. **Ранно предупреждение:** Изпраща се без неоправдано забавяне и във всички случаи **в срок до 24 часа** от узнаването за значителния инцидент;
2. **Доклад за инцидента:** Изпраща се под формата на официална актуализация с подробен анализ, оценка на щетите и предприети смекчаващи мерки **в срок до 72 часа** от узнаването за инцидента.

РАЗДЕЛ X. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Служителите в МГ „Гео Милев“ - Плевен са длъжни да познават и спазват разпоредбите, произтичащи от тези правила.

§ 2. Настоящите политика се разглежда и оценява периодично с оглед ефективността ѝ, като МГ „Гео Милев“ - Плевен може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 3. За всички неуредени случаи се прилагат разпоредбите на Регламент (ЕС) 2016/679 (GDPR), Закона за защита на личните данни и Кодекса на труда.

§ 4. Тази политика е разработена съгласно ЗАКОН ЗА КИБЕРСИГУРНОСТ и НАРЕДБА за минималните изисквания за мрежова и информационна сигурност и влиза в сила от датата на извеждане на Заповед № РД-11-1918/14.09.2026г. на директора на МГ „Гео Милев“ - Плевен.

Приложение 1

Таблица за отговорности и срокове на съхранение на видеозаписите

№	Дейност / Област	Отговорно лице	Срок на съхранение	Коментари / Забележки
1	Настройка и поддръжка на системата за видеонаблюдение	IT специалист от фирмата доставчик на услугата	Постоянно (за технически цели)	Включва поддръжка на камери, сървъри, архивиране
2	Съхранение на видеозаписите	Директор или упълномощено лице	До 15 календарни дни	Ако е образувано разследване – до приключване на случая
3	Предоставяне на достъп до видеозаписи на субекти на данни	Директор / упълномощено лице	При заявка	В съответствие с GDPR и ЗЗЛД; документиращ се предоставянето
4	Предоставяне на видеозаписи на държавни органи (МВР, прокуратура, съд)	Директор / упълномощено лице	До приключване на разследването	Исканията се съпровождат с официални документи
5	Контрол на преглед на видеозаписи с участие на трети лица	Директор / упълномощено лице	При преглед	Преглед на място, без разрешение за копиране или запис с лични устройства
6	Унищожаване на видеозаписи след изтичане на срока	Директор / упълномощено лице	Автоматично след 30 дни	Унищожаване по начин, недопускащ възстановяване
7	Информация и уведомяване на субектите на данни	Директор	Постоянно	Табели на входовете и в зони с видеонаблюдение, актуализиране при промяна на системата

Приложение 2

Образец!

Искане за достъп до лични данни от видеонаблюдение

До

Директора на Математическа гимназия „Гео Милев“ – гр. Плевен

От:.....

(трите имена на заявителя)

ЕГН:

Адрес:

Телефон/е-mail за връзка:

ИСКАНЕ

На основание чл. 15 от Регламент (ЕС) 2016/679 (GDPR) и чл. 5 от Правилата за видеонаблюдение в МГ „Гео Милев“ – Плевен, моля да ми бъде предоставен достъп до лични данни, свързани с видеозапис(и), на който/които съм заснет/а.

Описание на исканата информация (период, място, събитие):

.....

.....

.....

.....

.....

Предпочитана форма на достъп (преглед на място / копие на запис / писмена информация):

Дата:

Подпис:

Приложение 3

Образец!

ДЕКЛАРАЦИЯ

за съгласие при преглед на видеозапис

Долуподписаният/ата:

.....

(три имена на декларатора)

ЕГН:

Адрес:

В качеството ми на:

☐ Родител/настойник на ученик.....

☐ Служител в МГ „Гео Милев“ – гр. Плевен

ДЕКЛАРИРАМ, ЧЕ:

1. Давам своето съгласие да бъде извършен преглед на видеозапис от системата за видеонаблюдение на МГ „Гео Милев“ – гр. Плевен, на който съм (е) заснет/о моето дете, заедно с други лица.
2. Съгласен/на съм прегледът да се извърши в присъствието на всички засегнати лица/техните родители/настойници, на конкретна дата, определена от училището.
3. Декларирам, че няма да разгласявам, разпространявам или използвам по какъвто и да е начин информацията, станала ми известна при прегледа.
4. Запознат/а съм, че при прегледа не е допустимо да се извършва презапис или заснемане на видеозаписа с лични или други устройства.
5. Осведомен/а съм, че видеозаписите представляват лични данни по смисъла на Регламент (ЕС) 2016/679 (GDPR) и Закона за защита на личните данни.

Дата:

Подпис:

Приложение 4

ОПЕРАТИВЕН ПЛАН ЗА РЕАКЦИЯ ПРИ КИБЕРИНЦИДЕНТ (ПЪРВИТЕ 24 ЧАСА)

ЧАС 0- 1 (Първите 60 минути): Узнаване и Изолиране

Веднага след като служител, учител или ученик забележи признаци на инцидент (напр. блокиран достъп до електронния дневник, изтичане на лични данни в интернет и др.):

- **Незабавно докладване: Служителят уведомява устно и писмено Директора**
- **Спиране на заразата (Изолиране):** Ръководителят на направление „ИКТ“ незабавно изключва засегнатите компютри и сървъри от училищната мрежа (изваждане на LAN кабела или спиране на Wi-Fi).
- **Смяна на пароли:** Ръководителят на направление „ИКТ“ служебно нулира паролите на компрометираните профили и временно блокира външния достъп до училищния облак/сървър през VPN или отдалечен достъп.

ЧАС 1 – 4: Оценка на мащаба и Сформиране на щаб

- **Сформиране на Кризисен щаб:** Директорът свиква Щаб за реакция в състав: Директор, ръководител на направление „ИКТ“, Длъжностно лице по защита на данните и представител на външната ИТ фирма (ако има такава).
- **Първоначална класификация на инцидента:** Щабът определя дали инцидентът е „значителен“ съгласно ЗКС. Инцидентът е значителен, ако:
 - Прекъсва учебния или административния процес за повече от няколко часа.
 - Води до потенциална кражба или изтичане на чувствителни лични данни (ЕГН, оценки, медицински картони на ученици).
 - Засяга критична услуга, предоставена от външен доставчик (напр. масов срив в платформата за електронни дневници).

ЧАС 4 – 12: Техническо разследване и Събиране на доказателства

- **Логване и Архивиране (Logs):** Ръководител на направление „ИКТ“ извлича и записва на защитен външен носител всички системни дневници (logs) от

мрежовите устройства и сървъри, за да се разбере как е станал пробивът.

- **Оценка на щетите:** Проверява се целостта на резервните копия (backups). Установява се дали архивите са незасегнати и дали е възможно безопасно възстановяване на системите.
- **Комуникация с доставчици:** Ако пробивът е дошъл през външен софтуер или платформа, Директорът изпраща спешно писмено запитване до фирмата-доставчик за съдействие и изясняване на ситуацията.

ЧАС 12 – 20: Подготовка на известията

- **Попълване на бланката за CERT:** Директорът и ръководител на направление „ИКТ“ подготвят известието за **Ранно предупреждение**. То съдържа само базова информация:
 - Наименование и ЕИК на училището.
 - Време на откриване на инцидента.
 - Предполагам характер на атаката (напр. фишинг, зловреден софтуер, DDoS атака).
- Информация дали инцидентът има трансгранично въздействие
- **Оценка по GDPR:** Длъжностното лице по защита на данните (DPO) изготвя оценка дали има риск за правата на субектите (ученици, родители, учители). Ако има риск, започва подготовка на уведомление до Комисията за защита на личните данни (КЗЛД), за което срокът е до 72 часа.

ЧАС 20 – 24: Официално докладване (Краен срок по ЗКС)

- **Изпращане на Ранно предупреждение към CERT:** **Преди изтичането на 24-тия час** от узнаването, Директорът изпраща подготвеното съобщение към Националния CERT (към Министерството на електронното управление) по официалния електронен канал (обикновено чрез Системата за сигурно електронно връчване - ССЕВ или специализиран портал за инциденти).
- **Вътрешно информиране:** Директорът провежда оперативка с педагогическия и непедагогическия персонал. Дават се ясни указания какво да казват на родителите, ако има временни затруднения с учебния процес или електронните дневници. *Забранява се на служителите да коментират детайли по сигурността пред външни лица или медии без разрешение.*
- **Преход към Фаза 2:** Кризисният щаб набелязва стъпките за следващите 48 часа – подготовка на детайлния Окончателен доклад (до 72-рия час по ЗКС) и пълно възстановяване на дигиталната инфраструктура от сигурни архиви.