ДЕТСКА ГРАДИНА № 140 „ЗОРНИЦА“ с. ДОЛНИ БОГРОВ
✉ 1855, ул. 10, № 27, Район „Кремиковци”- СО
☎ тел. : 02/ 995 18 02, e-mail: info-2210673@ edu .mon.bg

УТВЪРЖДАВАМ: .....
/Десислава Петрова/

Заповед № 52/17.09.2026. г.

Политика за мрежова и информационна сигурност

на

ДГ № 140 “Зорница”

2026/2027 г.

ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

ДГ № 140 „Зорница“, с.Долни Богров за учебна 2026/2027г.

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Цел

Настоящата политика определя принципите, мерките и отговорностите за осигуряване на мрежова и информационна сигурност в ДГ № 140 „Зорница“, в съответствие с:

- Директива (ЕС) 2022/2555 (NIS2)
- Закон за киберсигурност
- Наредба № Н-1/03.05.2023 г.
- Регламент (ЕС) 2016/679 (GDPR)
- Закон за защита на личните данни
- вътрешните правила на СО и МОН

Политиката цели да гарантира:

- конфиденциалност
- цялост
- наличност
- непрекъсваемост
- реакция при инциденти
- съответствие с нормативните изисквания

II. ОБХВАТ

Политиката се прилага за:

- всички служители на ДГ № 140“Зорница“
- всички информационни системи и устройства
- всички данни, включително лични данни
- външни доставчици, които имат достъп до системи или информация

III. ИНФОРМАЦИОННИ АКТИВИ

Чл. 2. Активи на ДГ № 140“Зорница“

Категория	Описание
Хардуер	3 настолни компютъра, 6 лаптопа, 5 принтера
Мрежа	Кабелен интернет доставчик: **Пронет**, рутери, суичове, окабеляване
Софтуер	Електронен дневник **ЕДГ.БГ**, имейл **info-2210673@edu.mon.bg**, ССЕВ, офис пакети

Категория	Описание
Носители	USB устройства (служебни), външни дискове
Документация	Хартиена и електронна

IV. ОТГОВОРНОСТИ

Чл. 3. Директорът

- утвърждава политиката
- определя лице по сигурността
- осигурява обучение
- докладва инциденти
- извършва ежегоден преглед

Чл. 4. Лице по мрежова и информационна сигурност

- поддържа регистри
- следи за мерките
- организира тестове
- контролира достъпа
- участва в оценката на риска

Чл. 5. Служители

- използват системите само за служебни цели
- спазват правилата за достъп
- докладват инциденти
- не използват лични устройства за служебни данни

V. МЕРКИ ЗА СИГУРНОСТ

Чл. 6. Управление на достъпа

- уникални профили
- забрана за общи акаунти
- пароли със сложност
- смяна на 90 дни
- незабавно прекратяване при напускане

Чл. 7. Технически мерки

- антивирусна защита
- защитна стена
- автоматични актуализации
- резервни копия (седмично)
- криптиране

- логове

Чл. 8. Организационни мерки

- забрана за лични USB
- забрана за инсталиране на софтуер
- защита на мобилни устройства
- правила за работа от разстояние

Чл. 9. Външни доставчици

- клаузи за киберсигурност
- защита на данните
- право на одит
- отговорност при инциденти
- прозрачност на веригата на доставки (NIS2)

VI. УПРАВЛЕНИЕ НА РИСКА

Чл. 10. Оценка на риска

- ежегодно
- риск-регистър
- активи, заплахи, уязвимости, вероятност, въздействие, мерки

Чл. 11. План за третиране на риска

- мерки
- срокове
- отговорни лица
- ресурси

VII. ИНЦИДЕНТИ И НЕПРЕКЪСВАЕМОСТ

Чл. 12. Управление на инциденти

- незабавно докладване
- регистриране
- уведомяване на ГДБОП, ДАНС, СО, КЗЛД
- доклад и анализ

Чл. 13. Непрекъсваемост на дейността

- план за действие
- резервни копия
- процедури за възстановяване

- ежегодни тестове

VIII. ОБУЧЕНИЕ

Чл. 14. Обучение на персонала

- ежегодно обучение
- обучение при постъпване
- разпознаване на фишинг

IX. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 15. Преглед

Ежегоден или при промени в законодателството.

Чл. 16. Влизане в сила

От датата на утвърждаване.

ПРИЛОЖЕНИЕ 1

РЕГИСТЪР НА ИНФОРМАЦИОННИТЕ АКТИВИ

ДГ № 146 „Звездица“, гр. София

Версия: 1.0 **Дата:** 2026 г. **Отговорно лице:** ..... **Одобрил:** Директор Д.Петрова

1. Цел на регистъра

Регистърът съдържа всички информационни активи на ДГ № 140„Зорница“ съгласно изискванията на:

- Наредба № Н-1/03.05.2023 г.
- Закон за киберсигурност
- Директива NIS2
- GDPR

Той служи за: – оценка на риска – управление на инциденти – планиране на мерки за сигурност – контрол на достъпа – одити и проверки

2. Категории активи

Регистърът включва следните групи активи:

1. **Хардуерни устройства**
2. **Софтуер и информационни системи**
3. **Мрежова инфраструктура**
4. **Носители на информация**
5. **Документация**
6. **Процеси и дейности**
7. **Служители с достъп**
8. **Външни доставчици**

3. Таблица: Хардуерни активи

№	Актив	Количество	Локация	Отговорно лице	Критичност	Забележки
1	Настолни компютри	3	Администрация, групи	Лице по ИС	Средна	Служебни профили
2	Лаптопи	7	Администрация	Лице по ИС	Висока	Използват се за работа от разстояние
3	Принтери	10	Всички групи и администрация	Лице по ИС	Ниска	Някои са мрежови
4	Рутери	4	Администрация	Пронет / Лице по ИС	Висока	Основна мрежова свързаност
5	Суичове	3	Администрация	Лице по ИС	Висока	Вътрешна мрежа
6	UPS устройства	2	Администрация	Лице по ИС	Висока	Защита от токови удари

4. Таблица: Софтуер и информационни системи

№	Система / Софтуер	Описание	Собственик	Достъп	Критичност	Забележки
1	ЕДГ.БГ	Електронен дневник	МОН	Потребителски профили	Висока	Съдържа лични данни
2	ССЕВ	Система за	МОН	Профили	Висока	Задължителна за

№	Система / Софтуер	Описание	Собственик	Достъп	Критичност	Забележки
		отчетност				отчетност
3	Имейл info-22106673@edu.mon.bg	Официална комуникация	МОН	Директор, адм. служители	Висока	Съдържа чувствителна информация
4	Антивирусна защита	Защита на устройства	ДГ 140	Всички компютри	Висока	Автоматични актуализации
5	Офис пакет	Документи и отчети	ДГ 140	Администрация	Средна	Лицензиран

5. Таблица: Мрежова инфраструктура

№	Актив	Описание	Доставчик	Критичност	Забележки
1	Кабелен интернет	Основна интернет свързаност	Пронет	Висока	SLA по договор
2	Локална мрежа	Окабеляване, суичове	ДГ 140	Висока	Поддръжка от лице по ИС
3	Wi-Fi мрежа	Вътрешна мрежа	ДГ 140	Средна	За служебни устройства

6. Таблица: Носители на информация

№	Носител	Тип	Отговорно лице	Критичност	Забележки
1	USB памети	Служебни	Лице по ИС	Средна	Лични USB са забранени
2	Външни дискове	Backup	Лице по ИС	Висока	Седмични резервни копия

7. Таблица: Документация

№	Документ	Формат	Достъп	Критичност	Забележки
1	Политики и	Електронен/хартиен	Директор,	Висока	Актуализират се

№	Документ	Формат	Достъп	Критичност	Забележки
	процедури		лице по ИС		ежегодно
2	Регистри	Електронен	Лице по ИС	Висока	За проверки
3	Договори с доставчици	Хартиен	Директор	Средна	Съдържат клаузи за сигурност

8. Таблица: Процеси и дейности

№	Процес	Описание	Отговорник	Критичност
1	Обработка на лични данни	Данни за деца, родители, служители	Директор	Висока
2	Въвеждане на данни в ЕДГ.БГ	Дневници, отсъствия	Учители	Висока
3	Работа с ССЕВ	Отчети	Администрация	Висока
4	Имейл комуникация	Официална кореспонденция	Директор, адм. служители	Висока

9. Таблица: Служители с достъп

№	Длъжност	Ниво на достъп	Системи	Забележки
1	Директор	Пълен	Всички	Администратор
2	Зам.-директор	Разширен	ЕДГ.БГ, имейл	
3	Учители	Ограничен	ЕДГ.БГ	
4	Административни служители	Среден	Имейл, ССЕВ	
5	Лице по ИС	Администратор	Всички	Техническа поддръжка

10. Таблица: Външни доставчици

№	Доставчик	Услуга	Достъп до данни	Критичност	Забележки
1	Пронет	Интернет	Не	Висока	Мрежова свързаност
2	МОН	ЕДГ.БГ, ССЕВ,	Да	Висока	Национални

№	Доставчик	Услуга	Достъп до данни	Критичност	Забележки
		имейл			системи
3	Сервиз техника	Поддръжка	Ограничен	Средна	Достъп само при нужда

ПРИЛОЖЕНИЕ 2

РИСК-РЕГИСТЪР

ДГ № 140 „Зорница“,

Версия: 1.0 **Дата:** 2026 г. **Отговорно лице:** ..... **Одобрил:** Директор :Д.Петрова

1. Цел на риск-регистъра

Риск-регистърът служи за:

- идентифициране на заплахи
- оценка на вероятност и въздействие
- определяне на ниво на риск
- планиране на мерки за намаляване на риска
- изпълнение на изискванията на Наредба Н-1, NIS2 и Закона за киберсигурност

2. Методика за оценка

2.1. Скала за вероятност (1–5)

Стойност	Описание
1	Много малко вероятно
2	Малко вероятно
3	Възможно
4	Вероятно
5	Много вероятно

2.2. Скала за въздействие (1–5)

Стойност	Описание
1	Незначително
2	Малко
3	Средно

Стойност	Описание
4	Значително
5	Критично

2.3. Формула за риск

Риск = Вероятност × Въздействие

2.4. Нива на риск

Стойност	Ниво	Действие
1–5	Нисък	Приема се
6–12	Среден	Нужни мерки
13–25	Висок	Незабавни мерки

3. Риск-регистър (таблица)

Персонализиран за реалните активи на ДГ № 146.

3.1. Рискове за хардуер

Таблица 1 — Хардуерни активи

№	Актив	Заплаха	Уязвимост	Вер.	Възд.	Риск	Мерки	Отговорник
1	Настолни компютри (14)	Хардуерен отказ	Амортизация, стареене	3	4	12	Поддръжка, подмяна	Лице по ИС
2	Лаптопи (7)	Кражба	Мобилност	4	4	16	Заключване, съхранение	Директор
3	Принтери (10)	Неправомерен печат	Липса на контрол	3	2	6	Ограничен достъп	Адм. служител
4	Рутери/суичове	Отказ на мрежа	Токови удари	3	5	15	UPS, поддръжка	Лице по ИС
5	UPS	Повреда	Претоварване	2	4	8	Профилактика	Лице по ИС

3.2. Рискове за софтуер и системи

Таблица 2 — Софтуер и системи

№	Система	Заплаха	Уязвимост	Вер.	Възд.	Риск	Мерки	Отговорник
1	ЕДГ.БГ	Неправомерен достъп	Слаби пароли	3	5	15	Сложни пароли,	Учители

№	Система	Заплаха	Уязвимост	Вер.	Възд.	Риск	Мерки	Отговорник
							обучение	
2	ИССЕВ	Грешни данни	Човешка грешка	3	4	12	Двоен контрол	Адм. служител
3	Имейл	Фишинг	Липса на обучение	4	5	20	Обучение, филтри	Директор
4	Антивирус	Пропуск	Неактуализиран софтуер	2	5	10	Автоматични ъпдейти	Лице по ИС
5	Офис пакет	Загуба на данни	Липса на backup	3	4	12	Backup политика	Лице по ИС

3.3. Рискове за мрежова инфраструктура

Таблица 3 — Мрежа

№	Актив	Заплаха	Уязвимост	Вер.	Възд.	Риск	Мерки	Отговорник
1	Интернет (Пронет)	Прекъсване	Външна повреда	3	5	15	Договорен SLA	Директор
2	Wi-Fi	Неправомерен достъп	Слаба парола	4	4	16	WPA3, смяна на пароли	Лице по ИС
3	Локална мрежа	Вътрешна атака	Неправилен достъп	2	4	8	Ограничения по VLAN	Лице по ИС

3.4. Рискове за лични данни

Таблица 4 — Лични данни

№	Данни	Заплаха	Уязвимост	Вер.	Възд.	Риск	Мерки	Отговорник
1	Данни за деца	Изтичане	Грешка на служител	3	5	15	Обучение, контрол	Директор
2	Данни за родители	Неправомерен достъп	Слаби пароли	3	4	12	Политика за пароли	Учители
3	Данни за служители	Загуба	Липса на backup	2	4	8	Backup	Лице по ИС

3.5. Рискове за процеси

Таблица 5 — Процеси

№	Процес	Заплаха	Уязвимост	Вер.	Възд.	Риск	Мерки	Отговорник
1	Въвеждане в ЕДГ.БГ	Грешни данни	Човешка грешка	3	4	12	Двоен контрол	Учители

№	Процес	Заплаха	Уязвимост	Вер.	Възд.	Риск	Мерки	Отговорник
2	Имейл комуникация	Фишинг	Липса на обучение	4	5	20	Обучение	Директор
3	Документооборот	Загуба	Липса на архив	2	4	8	Архивиране	Адм. служител

3.6. Рискове от външни доставчици

Таблица 6 — Доставчици

№	Доставчик	Заплаха	Уязвимост	Вер.	Възд.	Риск	Мерки	Отговорник
1	Пронет	Прекъсване	Външни фактори	3	5	15	SLA, контакт	Директор
2	МОН	Системен отказ	Национални системи	2	5	10	Алтернативни канали	Директор
3	Сервиз техника	Неправомерен достъп	Физически достъп	2	4	8	Придружаване	Лице по ИС

4. План за третиране на рисковете

Таблица 7 — План за мерки

№	Риск	Ниво	Мярка	Срок	Отговорник
1	Фишинг атаки	Висок	Обучение	1 месец	Директор
2	Кражба на лаптоп	Висок	Заключване, сейф	1 месец	Лице по ИС
3	Прекъсване на интернет	Висок	SLA, резервен мобилен интернет	2 месеца	Директор
4	Слаби пароли	Среден	Политика за пароли	1 месец	Лице по ИС
5	Липса на backup	Среден	Backup политика	1 месец	Лице по ИС

ПРИЛОЖЕНИЕ 3

РЕГИСТЪР НА ИНЦИДЕНТИ ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

ДГ № 140 „Зорница“, с.Долни Богров

Версия: 1.0 **Дата:** 2026 г. **Отговорно лице:** ..... **Одобрил:** Директор

1. Цел на регистъра

Регистърът документира всички инциденти, свързани с мрежовата и информационната сигурност в ДГ № 146 „Звездица“, включително:

- нарушения на конфиденциалността
- нарушения на целостта
- нарушения на наличността
- технически откази
- човешки грешки
- опити за неоторизиран достъп
- фишинг, зловреден софтуер, пробиви
- инциденти с лични данни

Регистърът се поддържа съгласно Наредба Н-1, Закона за киберсигурност, NIS2 и GDPR.

2. Процедура за вписване

1. Всеки служител е длъжен незабавно да докладва инцидент.
2. Лицето по мрежова и информационна сигурност регистрира инцидента.
3. При инциденти с лични данни се уведомява КЗЛД.
4. При сериозни киберинциденти се уведомяват ГДБОП и ДАНС.
5. След отстраняване се вписват предприетите мерки и резултатът.

3. Таблица: Регистър на инциденти

№	Дата и час	Вид инцидент	Засегнати системи/устройства	Описание	Въздействие	Предприети действия	Уведомени органи	Отговорник	Статус
1		Неправомерен достъп	ЕДГ.БГ / имейл						
2		Фишинг опит	Имейл						
3		Хардуерен отказ	Компютър / лаптоп						

№	Дата и час	Вид инцидент	Засегнати системи/устройства	Описание	Въздействие	Предприети действия	Уведомени органи	Отговорник	Статус
4		Прекъсване на интернет	Мрежа (Пронет)						
5		Загуба на данни	Документи / ССЕВ						
6		Зловреден софтуер	Компютър						
7		Нарушение на лични данни	ЕДГ.БГ / документи						
8		Физически инцидент	Устройство						

4. Категории инциденти

4.1. Технически инциденти

- отказ на компютър
- отказ на принтер
- проблем с мрежово устройство
- прекъсване на интернет

4.2. Киберинциденти

- фишинг
- зловреден софтуер
- опит за пробив
- неоторизиран достъп

4.3. Инциденти с лични данни

- неправомерно разкриване
- изпращане на грешен получател
- загуба на документи
- грешно въведени данни

4.4. Човешки грешки

- изтриване на данни
- неправилно боравене с устройства
- грешно въвеждане в ЕДГ.БГ или ИССЕВ

5. Статуси на инцидентите

- **Отворен** – инцидентът е регистриран и се обработва
- **В процес на анализ** – извършва се проверка
- **Отстранен** – инцидентът е решен
- **Затворен** – приключен и документиран
- **Докладван** – изпратен към компетентни органи

6. Съхранение и достъп

- Регистърът се съхранява в електронен формат на защитено място.
- Достъп имат: директорът, лицето по ИС и проверяващи органи.
- Съхранява се минимум 5 години.

ПРИЛОЖЕНИЕ 4

ПЛАН ЗА НЕПРЕКЪСВАЕМОСТ НА ДЕЙНОСТТА (Business Continuity Plan)

ДГ № 146 „Звездица“, гр. София

Версия: 1.0 **Дата:** 2026 г. **Отговорно лице:** ..... **Одобрил:** Директор Д.Петрова

1. Цел на плана

Планът за непрекъсваемост на дейността определя действията, които ДГ № 146 „Звездица“ предприема при:

- прекъсване на интернет
- отказ на техника
- киберинциденти
- загуба на данни
- природни бедствия
- пожар, наводнение, токов удар
- недостъпност на национални системи (ЕДГ.БГ, ИССЕВ, имейл)

Целта е да се гарантира, че основните дейности на детската градина могат да продължат или да бъдат възстановени в максимално кратък срок.

2. Обхват

Планът се прилага за:

- всички служители
- всички информационни системи
- всички хардуерни устройства

- всички процеси, свързани с работа с данни
- всички помещения, в които се съхранява техника

3. Критични дейности

№	Дейност	Описание	Критичност	Максимално допустимо прекъсване
1	Въвеждане в ЕДГ.БГ	Дневници, отсъствия	Висока	24 часа
2	Имейл комуникация	Официална кореспонденция	Висока	24 часа
3	ССЕВ	Отчети	Висока	48 часа
4	Документооборот	Заповеди, протоколи	Средна	48 часа
5	Работа на администрацията	Оперативни задачи	Висока	24 часа

4. Потенциални сценарии и действия

4.1. Прекъсване на интернет (Пронет)

Симптоми: – липса на достъп до ЕДГ.БГ, ИССЕВ, имейл – липса на Wi-Fi

Действия:

1. Проверка на рутер/суич.
2. Рестарт на мрежовото оборудване.
3. Проверка на кабелни връзки.
4. Свързване с Пронет.
5. При продължителен проблем – използване на резервен мобилен интернет (телефон с hotspot).

Отговорник: Лице по ИС / Директор **Време за възстановяване:** до 2 часа

4.2. Отказ на компютър или лаптоп

Симптоми: – не стартира – замръзва – хардуерен шум

Действия:

1. Изключване и повторно включване.
2. Проверка на кабели и захранване.
3. Прехвърляне на работата на друг компютър.
4. Уведомяване на лице по ИС.
5. При нужда – сервиз.

Отговорник: Лице по ИС **Време за възстановяване:** до 24 часа

4.3. Загуба на данни

Симптоми: – изтрити файлове – повредени документи – липсваща информация

Действия:

1. Проверка на резервните копия.
2. Възстановяване от последния backup.
3. Докладване на инцидента.
4. Анализ на причината.

Отговорник: Лице по ИС **Време за възстановяване:** до 4 часа

4.4. Киберинцидент (фишинг, зловреден софтуер, пробив)

Симптоми: – подозрителни имейли – блокирани файлове – странно поведение на компютър

Действия:

1. Незабавно изключване на устройството от интернет.
2. Уведомяване на директора и лице по ИС.
3. Сканиране с антивирусна програма.
4. Докладване към ГДБОП/ДАНС при сериозен инцидент.
5. Възстановяване от backup при нужда.

Отговорник: Лице по ИС **Време за възстановяване:** до 24 часа

4.5. Пожар, наводнение, токов удар

Действия:

1. Евакуация на персонала и децата.
2. Изключване на електрическото захранване (ако е безопасно).
3. Уведомяване на компетентните служби.
4. Преглед на щетите.
5. Възстановяване на техниката, ако е възможно.
6. Използване на резервни устройства.

Отговорник: Директор **Време за възстановяване:** според щетите

5. Резервни ресурси

№	Ресурс	Описание	Локация	Отговорник
1	Резервен лаптоп	За спешни случаи	Администрация	Лице по ИС
2	Резервен мобилен интернет	Hotspot	Директор	Директор
3	Backup носители	Външни дискове	Заключен шкаф	Лице по ИС
4	Хартиени дневници	При отказ на ЕДГ.БГ	Администрация	Учители

6. Възстановяване на дейността

1. Оценка на щетите.
2. Приоритизиране на критичните дейности.
3. Възстановяване на системи по следния ред:
   - интернет
   - имейл
   - ЕДГ.БГ
   - ССЕВ
   - документооборот
4. Докладване на предприетите действия.
5. Анализ и актуализация на плана.

7. Тестове на плана

- Провеждат се минимум **веднъж годишно**.
- Документират се резултатите.
- При нужда планът се актуализира.

8. Съхранение и достъп

- Планът се съхранява в електронен и хартиен формат.
- Достъп имат директорът и лицето по ИС.
- Предоставя се при проверки от СО, МОН, КЗЛД, ДАНС.

ПРИЛОЖЕНИЕ 5

ПРОЦЕДУРА ЗА УПРАВЛЕНИЕ НА ИНЦИДЕНТИ ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

ДГ № 140 „Зорница“, с.Долни Богров

Версия: 1.0 **Дата:** 2026 г. **Отговорно лице:** ..... **Одобрил:** Директор Д.Петрова .

1. Цел на процедурата

Процедурата определя реда за:

- откриване
- докладване
- регистриране
- анализ
- овладяване
- възстановяване
- докладване към компетентни органи

на инциденти, свързани с мрежовата и информационната сигурност в ДГ № 146 „Звездица“.

2. Обхват

Процедурата се прилага за:

- всички служители
- всички информационни системи (ЕДГ.БГ, ИССЕВ, имейл)
- всички устройства (компютри, лаптопи, принтери, мрежово оборудване)
- всички данни, включително лични данни

3. Определения

Инцидент – всяко събитие, което застрашава:

- конфиденциалността
- целостта
- наличността
- нормалната работа на системите

Примери: – фишинг имейл – зловреден софтуер – неправомерен достъп – загуба на данни – хардуерен отказ – прекъсване на интернет – грешно изпратен имейл с лични данни

4. Роли и отговорности

4.1. Служители

- незабавно докладват инцидент
- не предприемат самостоятелни действия, които могат да влошат ситуацията
- сътрудничат при разследването

4.2. Лице по мрежова и информационна сигурност

- приема и регистрира инцидента
- анализира причините
- предприема технически мерки
- уведомява директора

- подготвя доклади

4.3. Директор

- взема решения за ескалация
- уведомява компетентните органи при нужда
- одобрява доклади и мерки

5. Етапи на управление на инцидент

5.1. Откриване

Инцидент може да бъде открит чрез:

- служител
- антивирусна система
- системни логове
- външен сигнал
- доставчик на услуга

5.2. Докладване

Инцидентът се докладва незабавно на:

Лице по мрежова и информационна сигурност или **Директора**

Докладването може да бъде:

- устно
- по телефон
- по имейл
- чрез запис в регистъра

5.3. Регистриране

Инцидентът се вписва в **Регистъра на инциденти** (Приложение 3).

5.4. Анализ

Лицето по ИС извършва:

- определяне на вида инцидент
- оценка на въздействието
- оценка на риска
- идентифициране на засегнатите системи

5.5. Овладяване

В зависимост от инцидента:

- изключване на устройство от мрежата
- блокиране на акаунт
- смяна на парола
- спиране на услуга
- изолиране на заразен компютър
- временно преминаване към хартиени дневници

5.6. Възстановяване

- възстановяване от резервни копия
- рестартиране на системи
- повторно активиране на услуги
- проверка за остатъчни рискове

5.7. Докладване към външни органи

При нужда се уведомяват:

- **ГДБОП – Киберпрестъпност**
- **ДАНС**
- **КЗЛД** (ако има лични данни)
- **СО / МОН**

5.8. Доклад и заключение

Изготвя се доклад, който съдържа:

- описание на инцидента
- предприети действия
- резултат
- препоръки
- мерки за предотвратяване

6. Категоризация на инциденти

Категория	Описание	Примери
Нисък	Минимално въздействие	Отказ на принтер
Среден	Влияе на работа	Прекъсване на интернет
Висок	Засяга лични данни	Грешно изпратен имейл
Критичен	Засяга много системи	Зловреден софтуер, пробив

7. Време за реакция

Ниво	Време за реакция	Пример
Нисък	до 24 часа	Проблем с принтер
Среден	до 4 часа	Прекъсване на интернет
Висок	до 1 час	Грешно изпратени лични данни
Критичен	незабавно	Зловреден софтуер, пробив

8. Съхранение на информация

- Докладите и регистърът се съхраняват минимум 5 години.
- Достъп имат директорът и лицето по ИС.

9. Актуализация

Процедурата се актуализира:

- ежегодно
- при промени в законодателството
- след сериозен инцидент

ПРИЛОЖЕНИЕ 6

ПРОЦЕДУРА ЗА УПРАВЛЕНИЕ НА ДОСТЪПА ДО ИНФОРМАЦИОННИТЕ СИСТЕМИ И АКТИВИ

ДГ № 140 „Зорница“, гр. София

Версия: 1.0 **Дата:** 2026 г. **Отговорно лице:** ..... **Одобрил:** Директор Д.Петрова

1. Цел на процедурата

Процедурата определя правилата за:

- предоставяне на достъп
- промяна на достъп
- прекратяване на достъп
- контрол върху достъпа
- защита на потребителските профили
- управление на пароли

към информационните системи, устройствата и данните в ДГ № 140 „Зорница“.

2. Обхват

Процедурата се прилага за:

- всички служители
- всички системи (ЕДГ.БГ, ИССЕВ, имейл, вътрешни документи)
- всички устройства (компютри, лаптопи, мрежови устройства)
- всички потребителски профили
- външни лица, когато им се предоставя временен достъп

3. Основни принципи

1. Достъпът се предоставя **само при необходимост** за изпълнение на служебни задължения.
2. Всеки служител използва **уникален потребителски профил**.
3. Забранено е използването на **общи акаунти**.
4. Достъпът се предоставя по принципа **„минимални права“**.
5. Достъпът се прекратява **незабавно** при напускане или промяна на длъжност.
6. Паролите се пазят като **строго поверителна информация**.

4. Процедура за предоставяне на достъп

4.1. Иницииране

Достъп се предоставя:

- при назначаване на нов служител
- при промяна на длъжност
- при необходимост от допълнителни права

Инициира се от:

- директора
- лице по ИС
- административен служител (за ИССЕВ)

4.2. Създаване на профил

Лице по ИС създава профил в:

- компютърната система
- имейл (ако е необходимо)
- ЕДГ.БГ (по заявка от директора)
- ИССЕВ (по заявка от директора)

4.3. Определяне на права

Права се определят според длъжността:

Длъжност	Права
Директор	Пълен достъп
Зам.-директор	Разширен достъп
Учители	Достъп до ЕДГ.БГ
Административни служители	Имейл, ИССЕВ
Лице по ИС	Администраторски права

4.4. Документиране

Всяко предоставяне на достъп се вписва в:

- Регистър на достъпите (част от регистъра на активите)

5. Процедура за промяна на достъп

Промяна се извършва при:

- промяна на длъжност
- разширяване на отговорности
- ограничаване на права

Стъпки:

1. Директорът подава заявка към лице по ИС.
2. Лице по ИС променя правата.
3. Промяната се вписва в регистъра.

6. Процедура за прекратяване на достъп

Прекратяване се извършва при:

- напускане
- преместване
- дисциплинарни причини
- риск за сигурността

Стъпки:

1. Директорът уведомява лице по ИС.
2. Лице по ИС незабавно:
    - деактивира профила
    - премахва достъп до имейл
    - премахва достъп до ЕДГ.БГ

- премахва достъп до ИССЕВ

3. Действието се вписва в регистъра.

7. Политика за пароли

1. Минимална дължина: **8 символа.**
2. Съдържа:
   - главна буква
   - малка буква
   - цифра
   - специален символ
3. Паролите се сменят **на всеки 90 дни.**
4. Забранено е:
   - записване на пароли на лист
   - споделяне на пароли
   - използване на една и съща парола за лични и служебни профили

8. Контрол на достъпа

1. Достъпът до помещения с техника е ограничен.
2. Лаптопите се съхраняват заключени.
3. USB устройства са само служебни.
4. Wi-Fi достъпът е защитен с WPA3 и сложна парола.
5. Логовете за достъп се преглеждат периодично.

9. Временен достъп

Временен достъп се предоставя само при:

- сервизна дейност
- инсталация
- поддръжка

Условия:

- достъпът е ограничен
- служител придружава външното лице
- достъпът се прекратява веднага след приключване

10. Нарушения

Нарушения на правилата за достъп водят до:

- ограничаване на права
- дисциплинарни мерки
- докладване към директора

- при нужда – докладване към компетентни органи

11. Актуализация

Процедурата се актуализира:

- ежегодно
- при промени в законодателството
- при инцидент, свързан с достъп

ПРИЛОЖЕНИЕ 7

ПРОЦЕДУРА ЗА РЕЗЕРВНИ КОПИЯ (BACKUP POLICY)

ДГ № 140 „Зорница“, с.Долни Богров

Версия: 1.0 **Дата:** 2026 г. **Отговорно лице:** ..... **Одобрил:** Директор Д.Петрова

1. Цел на процедурата

Процедурата определя правилата за:

- създаване на резервни копия (backup)
- съхранение на резервни копия
- възстановяване на данни
- контрол и тестване на backup процесите

Целта е да се гарантира, че данните на ДГ № 140„Зорница“ могат да бъдат възстановени при:

- хардуерен отказ
- човешка грешка
- киберинцидент
- загуба или повреда на данни
- бедствия или аварии

2. Обхват

Процедурата се прилага за:

- всички електронни документи
- данни в ЕДГ.БГ (възстановяват се чрез МОН)
- данни в ИССЕВ (възстановяват се чрез МОН)
- имейл кореспонденция
- локални файлове на компютри и лаптопи

- служебни USB носители
- външни дискове за backup

3. Видове резервни копия

3.1. Пълно резервно копие

Съдържа всички важни файлове и документи.

Извършва се: **веднъж седмично.**

3.2. Инкрементално резервно копие

Съдържа само променените файлове.

Извършва се: **ежедневно (ако има промени).**

3.3. Резервни копия на имейл

Имейлът в домейна **edu.mon.bg** се архивира автоматично от МОН.

3.4. Резервни копия на национални системи

ЕДГ.БГ и ИССЕВ се архивират от МОН и не изискват локален backup.

4. Отговорности

Роля	Отговорности
Лице по ИС	Извършва backup, съхранява носителите, тества възстановяване
Директор	Контролира процеса, одобрява политики
Административни служители	Предоставят файлове за архивиране при нужда

5. Процедура за създаване на резервни копия

5.1. Подготовка

1. Проверка на външния диск за повреди.
2. Проверка на наличното пространство.
3. Проверка за вируси на компютъра.

5.2. Извършване на backup

1. Архивиране на:

    - документи на администрацията
    - електронни протоколи
    - отчети
    - вътрешни регистри
    - файлове, свързани с дейността на ДГ
2. Копиране на данните на външен диск.
3. Проверка дали файловете са копирани успешно.

5.3. Съхранение

Резервните копия се съхраняват:

- на **външен диск**,
- в **заключен шкаф**,
- с достъп само за директора и лицето по ИС.

6. Процедура за възстановяване на данни

6.1. Иницииране

Възстановяване се извършва при:

- загуба на данни
- повредени файлове
- киберинцидент
- хардуерен отказ

6.2. Стъпки

1. Идентифициране на липсващите/повредени данни.
2. Избор на подходящо резервно копие.
3. Възстановяване на файловете.
4. Проверка на целостта на възстановените данни.
5. Документиране в регистъра на инциденти (ако е инцидент).

7. Тестове на резервните копия

Тестове се извършват:

- **веднъж на 6 месеца**
- чрез възстановяване на примерни файлове

Документират се:

- дата
- резултат

- проблеми
- препоръки

8. Съхранение и защита на backup носителите

1. Backup носителите се съхраняват в заключен шкаф.
2. Достъп имат само директорът и лице по ИС.
3. Носителите се подменят на всеки **2 години** или при повреда.
4. Забранено е използването на лични USB устройства.

9. Сигурност

- Backup файловете не се изпращат по имейл.
- Backup носителите не се изнасят извън сградата без разрешение.
- Backup файловете не се съхраняват в облачни услуги, които не са одобрени от МОН или СО.

10. Актуализация

Процедурата се актуализира:

- ежегодно
- при промени в инфраструктурата
- след инцидент, свързан с данни

ПРИЛОЖЕНИЕ 8

ПРОЦЕДУРА ЗА РАБОТА С ВЪНШНИ ДОСТАВЧИЦИ И ТРЕТИ СТРАНИ

ДГ № 140 „Зорница“, с.Долни Богров

Версия: 1.0 **Дата:** 2026 г. **Отговорно лице:** ..... **Одобрил:** Директор Д.Петрова

1. Цел на процедурата

Процедурата определя правилата за:

- избор на външни доставчици
- контрол върху достъпа им до информационни активи
- изисквания за сигурност към трети страни
- управление на рисковете, свързани с доставчици
- документиране на взаимоотношенията

Процедурата е съобразена с Наредба Н-1, NIS2, Закона за киберсигурност и GDPR.

2. Обхват

Процедурата се прилага за всички външни лица и организации, които:

- предоставят услуги
- извършват поддръжка
- имат достъп до техника
- имат достъп до помещения
- имат достъп до информация или системи

Примери: – интернет доставчик (Пронет) – сервиз за техника – МОН (ЕДГ.БГ, ИССЕВ, имейл) – външни фирми за ремонт

3. Категории доставчици

Категория	Примери	Ниво на риск
Доставчици на ИТ услуги	Пронет, сервиз техника	Висок
Доставчици на софтуер	МОН (ЕДГ.БГ, ИССЕВ)	Висок
Доставчици на оборудване	Компютърни фирми	Среден
Доставчици на поддръжка	Техници, ремонтни фирми	Среден
Доставчици без достъп до данни	Курири, доставчици	Нисък

4. Изисквания към външни доставчици

4.1. Договорни изисквания

Всеки договор с доставчик трябва да съдържа:

- клаузи за мрежова и информационна сигурност
- задължение за защита на личните данни
- забрана за копиране, изнасяне или разпространение на информация
- изискване за конфиденциалност
- изискване за прозрачност на веригата на доставки (NIS2)
- право на одит от страна на ДГ № 140“Зорница“
- отговорност при инциденти
- срокове за реакция при проблем

4.2. Технически изисквания

Доставчикът трябва да:

- използва защитени устройства
- спазва политиките на ДГ № 140“Зорница“
- работи само под наблюдение
- не използва лични USB устройства

- не инсталира софтуер без разрешение

5. Процедура за предоставяне на достъп на външни лица

5.1. Иницииране

Достъп се предоставя само:

- при необходимост
- след разрешение от директора

5.2. Регистрация

Външното лице се вписва в:

- дневник за посещения
- регистър за достъп на външни лица

5.3. Придружаване

Външните лица **не могат да бъдат оставяни без надзор.**

Придружават се от:

- лице по ИС или
- директор

5.4. Ограничаване на достъпа

Достъпът се ограничава до:

- конкретно помещение
- конкретно устройство
- конкретна задача

5.5. Прекратяване на достъпа

След приключване:

- достъпът се прекратява незабавно
- действията се вписват в регистъра
- проверява се дали няма оставени файлове, устройства или следи

6. Оценка на риска от доставчици

Оценката включва:

- вид услуга
- ниво на достъп
- възможни заплахи
- уязвимости
- мерки за контрол

Пример:

Доставчик	Риск	Ниво	Мерки
Пронет	Прекъсване на интернет	Висок	SLA, резервен интернет
Сервиз техника	Неправомерен достъп	Среден	Придружаване
МОН	Системен отказ	Висок	Алтернативни канали

7. Инциденти, свързани с доставчици

При инцидент:

1. Достъпът на доставчика се прекратява.
2. Инцидентът се вписва в регистъра.
3. Директорът уведомява компетентните органи при нужда.
4. Доставчикът носи отговорност според договора.

8. Забранени действия за външни лица

- използване на лични устройства
- копиране на данни
- снимане на екрани или документи
- достъп до Wi-Fi без разрешение
- инсталиране на софтуер
- изнасяне на техника

9. Съхранение и контрол

- Документите за доставчици се съхраняват в администрацията.
- Достъп имат директорът и лице по ИС.
- Преглеждат се ежегодно.

10. Актуализация

Процедурата се актуализира:

- ежегодно
- при промени в законодателството
- при промяна на доставчик
- след инцидент

ПРИЛОЖЕНИЕ 9

ПРОГРАМА ЗА ОБУЧЕНИЕ И ОСВЕДОМЕНОСТ НА ПЕРСОНАЛА ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

ДГ № 146 „Звездица“, гр. София

Версия: 1.0 **Дата:** 2026 г. **Отговорно лице:** ..... **Одобрил:** Директор Ст. Николова

1. Цел на програмата

Програмата има за цел:

- повишаване на знанията и уменията на персонала
- намаляване на риска от човешки грешки
- разпознаване на киберзаплахи
- правилно боравене с лични данни
- спазване на вътрешните политики
- изпълнение на изискванията на Наредба Н-1, NIS2, GDPR и Закона за киберсигурност

2. Обхват

Програмата се прилага за:

- директор
- зам.-директор
- учители
- административни служители
- помощен персонал (в частта за обща осведоменост)
- външни лица при необходимост

3. Видове обучения

3.1. Въвеждащо обучение (при постъпване на работа)

Всеки нов служител преминава обучение, което включва:

- правила за достъп
- работа с ЕДГ.БГ
- работа с имейл
- защита на лични данни
- разпознаване на фишинг
- работа с устройства
- забранени действия

3.2. Годишно обучение

Провежда се веднъж годишно и включва:

- актуални заплахи
- нови изисквания
- анализ на инциденти от годината
- добри практики
- тест за проверка на знанията

3.3. Тематични обучения

Провеждат се при нужда:

- промени в законодателството
- нови системи (напр. актуализации на ЕДГ.БГ)
- след инцидент

4. Теми на обучението

4.1. Основни теми

- Какво е мрежова и информационна сигурност
- Какво е лични данни и как се защитават
- Какво е фишинг и как се разпознава
- Какво е зловреден софтуер
- Какво е инцидент и как се докладва
- Как се работи безопасно с имейл
- Как се използват пароли
- Как се работи с ЕДГ.БГ и ИССЕВ безопасно
- Как се съхраняват документи

4.2. Практически модули

- Разпознаване на фишинг имейли
- Симулирани атаки (примерни фишинг съобщения)
- Работа с резервни копия
- Правилно заключване на устройства
- Реакция при инцидент

5. График на обученията

Вид обучение	Периодичност	Отговорник	Участници
Въвеждащо	При постъпване	Директор / Лице по ИС	Нови служители
Годишно	Веднъж	Директор	Всички служители

Вид обучение	Периодичност	Отговорник	Участници
	годишно		
Тематично	При нужда	Лице по ИС	Определени служители
Обучение по лични данни	Веднъж годишно	Директор	Всички служители
Обучение по киберсигурност	Веднъж годишно	Лице по ИС	Всички служители

6. Материали за обучение

- презентации
- видеоматериали
- ръководства
- вътрешни инструкции
- тестове
- примерни фишинг имейли
- казуси

7. Документиране

За всяко обучение се води:

- присъствен списък
- протокол
- материали от обучението
- тестове (ако има)
- оценка на резултатите

Документите се съхраняват минимум 5 години.

8. Оценка на ефективността

Ефективността се оценява чрез:

- тестове
- анализ на инциденти
- обратна връзка от служителите
- проверки от директора

При нужда програмата се актуализира.

9. Актуализация

Програмата се актуализира:

- ежегодно
- при промени в законодателството
- при промяна на системите
- след инцидент