ДЕТСКА ГРАДИНА № 40 „ПРОФ. Д-Р Г. АНГУШЕВ“, СО РАЙОН „ТРИАДИЦА”
гр.София 1404, ул. „Метличина поляна“ № 10, тел.: 02/ 859 1115 e-mail:
cdg_40@abv.bg; www.dg40-angushev.com

УТВЪРЖДАВАМ:
ДИРЕКТОР НА ДГ № 40 „ПРОФ. Д-Р Г. АНГУШЕВ“
ВЕСЕЛИНА ГЕОРГИЕВА
Със Заповед № РД-15-87-52/ 25.09.2026 г.
В сила от 25.09.2026 г.



ПОЛИТИКА
ЗА
ИНФОРМАЦИОННАТА СИГУРНОСТ
НА
ДЕТСКА ГРАДИНА № 40 „ПРОФ. Д-Р Г. АНГУШЕВ“

1. Въведение
Настоящата политика за информационна сигурност е основополагащ документ, който дефинира насоките за защита на информацията и активите на детската градина. Политиката има за цел да:

- Осигури защита на чувствителни данни, включително лични данни на децата/родителите, учителите, административен персонал и посетители.
- Предотврати загуба, злоупотреба или неоторизиран достъп до информационните активи.
- Създаде култура на осведоменост за значението на информационната сигурност сред всички заинтересовани страни.

2. Цели на политиката
Целите на политиката включват:

- Установяване на систематичен подход за управление на информационната сигурност като част от процесите в него.
- Гарантиране на защитата на личните данни съгласно Регламент (ЕС) 2016/679 (GDPR).
- Намаляване на рисковете от външни атаки (включително кибератаки), човешки грешки или технически неизправности.

3. Обхват
Политиката обхваща:

- **Информационни активи**: Хардуер (компютри, сървъри, мрежово оборудване), софтуер (операционни системи, учебни платформи), хартиени документи и архиви.
- **Персонал**: Учители, административен персонал, и външни доставчици.
- **Процеси**: Управление на достъпа, обработка на данни, архивиране и управление на инциденти.

4. Основни принципи

4.1. **Конфиденциалност**

- Ограничаване на достъпа до информация само за упълномощени лица.
- Защита на личните данни чрез криптиране и контрол на достъпа.

4.2. **Цялостност**

- Гарантиране, че данните не са били модифицирани без разрешение.
- Използване на резервни копия за възстановяване на информация при необходимост.

4.3. **Наличност**

- Осигуряване на достъп до системите и информацията при нужда, чрез редовна поддръжка и резервиране на ресурси.

4.4. **Спазване на нормативни изисквания**

- Следене за съответствие с всички закони и регулации, свързани с информационна сигурност, както и обработката и защита на лични данни.

5. Роли и отговорности

5.1. Ръководство на детската градина

- Отговаря за цялостната рамка на информационна сигурност
- Осигурява ресурси за прилагане на политиката
- Одобрява стратегиите за информационна сигурност и защита на личните данни
- Получава доклади и статус за развитието на информационната сигурност и защита на личните данни , както и издава препоръки за подобрение

5.2. Отговорник по информационна сигурност (ОИС)

- Контролира спазването на политиката.
- Организира обучения и реагира при инциденти.
- Периодично докладва на ръководството.

5.3. Преподаватели и персонал

- Спазват изискванията за сигурност.
- Докладват за инциденти или подозрения за компрометиране на системи.

6. Управление на активи:

6.1. Идентификация и инвентаризация на активи

Всички активи на детската градина трябва да бъдат вписани в централен регистър, който включва следната информация:

- Описание на актива.
- Местоположение на актива.
- Отговорно лице или отдел.
- Категория и стойност на актива.
- Ниво на чувствителност и класификация

Активите се класифицират според тяхната чувствителност и значимост:
1. Критични активи: Лични данни, учебни и административни системи, които изискват най-висока степен на защита.
2. Служебни активи: Компютри, мрежово оборудване, които са необходими за ежедневната работа.
3. Общи активи: Публична информация, която не изисква строга защита.

Всеки актив трябва да има определено отговорно лице (собственик на актива), което:

- Носи отговорност за поддържането и защитата на актива.
- Осигурява правилното използване и съхранение.
- Докладва за възникнали проблеми или рискове.

Отговорното лице се назначава от ръководството на детската градина.
4. Разписва се документ за допустимо използване на активи, свързани с информацията и средствата за обработване на информация е документирано и описано в длъжностната характеристика на съответния служител.
5. Връщане на активи - всички служители и при прекратяване на тяхното трудово правоотношение, договор или споразумение трябва да върнат всички употребявани от тях активи на детската градина.

6.2 Защита на активите

6.2.1. Физическа защита:

- Заключване на помещенията със сървъри и оборудване. контрол на достъпа до физически архиви.

6.2.2. Техническа защита:

- Използване на антивирусни програми, защитни стени и системи за криптиране.
- Редовно архивиране на данните
- Управление на сменяеми външни носители – използването на сменяемите носители е силно ограничено. Извършва се мониторинг какви сменяеми носители се използват и каква информация се копира. Трябва да се използва специализиран софтуер за управление и мониторинг против изтичане на лични данни и чувствителна информация. Информацията върху сменяемите външни носители трябва да бъде криптирана чрез специализиран софтуер.

6.2.3 Административна защита:

- Определяне на нива на достъп за служители, в зависимост от тяхната роля.
- Подписване на декларации за конфиденциалност от персонала.

6.2.4 Извеждане от употреба и унищожаване

При изваждане на активи от употреба се предприемат следните стъпки:

- Изтриване на данни от цифровите носители чрез сертифицирани методи за унищожаване.
- Унищожаване на хартиени документи чрез шредиране.
- Собственикът на актива носи отговорност за правилното унищожаване или рециклиране.

7. Управление на логически достъп

- Всички информационни системи на детската градина следва да бъдат защитени с комплексни пароли
- Всички потребители получават индивидуални акаунти, защитени с пароли, които се сменят на всеки 90 дни.
- Достъпът до чувствителни данни се дава само на база "необходимост да знае".
- Автоматично заключване на акаунтите при 5 неуспешни опита за вход.
- Регулярно преразглеждане на списъците с права за достъп (кой потребител има достъп в системата и дали той все още е необходим).
- При отпадане на нужда от достъп (напускане на потребител, смяна на отговорности) , той се спира незабавно.
    - Отговорности при прекратяване или промяна на трудовото правоотношение на служители с достъп до информация - при напускане на служител, имащ достъп до информационни систем и/или обработващ лични данни, се предприемат действия по ограничаване на достъпа му до системи обработващи лични данни, както и физическия му достъп до помещения, в които се съхраняват лични данни. Отговорността за това носи ОИС. Следва

незабавно да бъдат сменени всички общодостъпни пароли, които се използват от много служители – пароли за Wi-Fi и други еднотипни пароли.

8. Класификация на информацията

8.1. Категории информация

- Обща информация:
- Вътрешна информация
- Чувствителна информация
- Критична информация

8.2. Маркиране на информацията

Всички документи следва да се маркират според класификацията си, като по-долу са изредени примери за това:

8.2.1 Обща (публична) информация

Примерен контекст:

- Графици за учебни дейности, които са публично достъпни.
- Обяви за събития и кампании на детската градина .
- Общи учебни материали, предназначени за децата.

Мерки за защита:

- Достъпни за всички, без специални ограничения.

8.2.2 Вътрешна информация

Примерен контекст:

- Вътрешни разпореждания и инструкции за преподаватели и служители.
- Работни графици на преподавателите.
- Статистически данни за резултати от учебния процес (без идентифицираща информация).

Мерки за защита:

- Ограничен достъп само за преподаватели и административен персонал.
- Задължително защита с пароли при дигитално съхранение.

8.2.3 Чувствителна информация

Примерен контекст:

- Лични данни на деца и родители (имена, адреси, контактни данни).
- Медицински документи на деца (ТЕЛК, здравни бележки и др), ако се съхраняват в детската градина .
- Бележки за доходи на родители
- Оценки и индивидуални доклади.

Мерки за защита:

- Криптиране при съхранение на цифрови носители.
- Физическо заключване на шкафове с хартиени копия.
- Контрол на достъпа на принципа "необходимост да знае" (напр. достъп само за администрация).

8.2.4 Критична информация

Примерен контекст:

- Системи за управление на данните на децата.

- Резервни копия на базата данни на детската градина .
- Документи, свързани с вътрешни разследвания или дисциплинарни действия.

Мерки за защита:

- Силно криптиране и редовно актуализиране на защитните системи.
- Съхранение на отделно физическо или облачно място с ограничен достъп.
- Редовни тестове за сигурността на системите.

9. Физическа сигурност и сигурност на заобикалящата среда

9.1 Сигурни зони - да се предотврати неоторизиран физически достъп, вреда и вмешателство в информацията и средствата за обработване на информация на детската градина .

- Граници за физическа сигурност - за защита на зони, които съдържат или чувствителна, или критична информация и средства за обработване на информация, се определят и използват граници за сигурност.
- Механизми за контрол на физическо влизане – добра практика е сигурните зони да бъдат защитени със съответни механизми за контрол на влизане, за да се гарантира, че само оторизираният персонал има разрешен достъп.
- Осигуряване на офиси, зали и съоръжения - трябва да бъде проектирана и приложена физическа защита за офиси, зали и съоръжения.
- Защита от външни заплахи и заплахи от околната среда - трябва да бъде проектирана и приложена физическа защита от природни бедствия, злонамерени атаки или инциденти.
- Работа в сигурни зони – трябва да се дефинират служителите, които имат достъп до помещенията, които са определени за сигурна зона.

9.2 Управление на устройства с да се предотвратят загуби, повреди, кражби или излагане на риск на активите и прекъсване на дейностите на детската градина.

- Устройствата са разположени и защитени, така че да се намалят рисковете от заплахи и опасности от околната среда и възможности за неоторизиран достъп. Сървърите трябва да бъдат поставени в специални обособени сървърни помещения, които да са с подходяща климатизация и вентилация. През помещенията не трябва да минават канализационни тръби или тръбни водни трасета. Помещенията трябва да разполагат с противопожарна система. Достъпът до помещенията трябва да бъде силно ограничен.
- Поддържащи комунални системи - устройствата трябва да бъдат защитени от повреди в електрозахранването и други разриви, предизвикани от откази в поддържащите комунални системи. Сървърите трябва да разполагат с онлайн UPS за резервиране на захранването.
- Сигурност на окабеляването - окабеляването за електрозахранване и телекомуникации, носещо данни или поддържащо информационни услуги, трябва да бъде защитено от подслушване, смущения или повреда и да бъде поставено в среда с ограничен достъп.
- Изнасяне на собственост и активи - устройства, информация или софтуер не се изнасят извън детската градина без предварително разрешение.
- Сигурност на устройства и активи извън помещенията - сигурността трябва да бъде прилагана и към активи, които са извън детската градина , като се отчитат различните рискове при работа извън помещенията на детската градина .

- Сигурно унищожаване или повторно използване на устройства - всички елементи на устройство, съдържащо запаметяващи носители, са проверявани, за да се гарантира, че всякакви чувствителни данни и лицензиран софтуер са премахнати или сигурно презаписани преди унищожаването или повторното използване.
- Потребителски устройства без надзор - потребителите трябва да осигурят оставените без надзор устройства да са подходящо защитени. Потребителите трябва да заключват работния екран на компютъра при напускане на работното място и функцията за автоматично заключване трябва да бъде активирана.
- Политика за чисто бюро и чист екран – при напускане на работното помещение всеки служител премахва всички хартиени носители от бюрото си, които съдържат лични данни. Работният екран на компютъра следва да бъде заключен при напускане на работното място и да се заключват шкафове, съдържащи хартиени копия на чувствителна информация.
- С цел наблюдение и отчетност следва да се използват системи за видеонаблюдение в ключови зони, като за използването им следва да се разпише политика (уведомление) към субектите на данни.

10. Защита на мрежата

Мрежовата инфраструктура на детската градина е критичен компонент за функционирането на информационните ú системи. Затова се прилагат следните мерки за защита на мрежата:

10.1. Сегментиране на мрежата
Мрежата се разделя на зони, включително:
- Учителска зона: За учители и административен персонал.
- Зона за гости: Изолирана от вътрешните ресурси на детската градина.

Зоните се управляват чрез виртуални локални мрежи (VLAN).
10.2. Контрол на достъпа до мрежата
- Неоторизираните устройства нямат достъп до мрежата.
- Всички устройства трябва да бъдат предварително регистрирани.
- Достъпът до мрежата се осъществява чрез защитен протокол (напр. WPA3 за Wi-Fi).

10.3. Мониторинг и откриване на аномалии
- Инсталират се системи за откриване на прониквания (IDS/IPS), които наблюдават мрежовия трафик и алармират при подозрителна активност.
- Записите (логовет за мрежовия трафик се съхраняват за минимум 1 месец за целите на анализ и разследване.

10.4. Защита на интернет връзката
- Използва се защитна стена (firewall), която ограничава достъпа до определени уебсайтове (например неподходящи или несигурни ресурси).
- Всички крайни устройства (компютри, лаптопи) следва да имат легален софтуер с инсталирани последни антивирусни дефиниции
- Всички устройства, свързани към мрежата, трябва да имат актуализиран антивирусен софтуер.

10.5. Криптиране на данни в мрежата

- Вътрешната комуникация между системите се криптира чрез SSL/TLS.
- При изпращане на чувствителна информация по мрежата се използва само криптиран канал.

11. Управление на инциденти

- Управление на инциденти и подобряване на сигурността на информацията – осигурен е последователен и ефикасен подход към управление на инцидентите със сигурността на информацията, включително съобщаване за събития и слабости, свързани със сигурността.
    - Отговорности и процедури – установени са отговорности и процедури за управление, за да се осигури бърза, ефикасна и системна реакция на инцидентите със сигурността на информацията.
    - Създаване на формален план за реагиране при инциденти, включващ:
        - Събиране на информация за инцидента.
        - Ограничаване на щетите.
        - Предприемане на корективни мерки.
        - Изготвяне на доклад с описание на причините за инцидента и предприемане на стъпки да не се допусне повторен такъв
    - Оценяване на събития, свързани със сигурността на информацията и вземане на решения за тях – събитията, свързани със сигурността на информацията, трябва да бъдат оценени, като трябва да бъде решено дали те трябва да бъдат класифицирани като инциденти със сигурността.
    - Докладване за събития свързани със сигурността на информацията– всички събития, свързани със сигурността на информацията (като кибератаки, загуба на данни, физическа кражба на оборудване и други свързани) , биват докладвани на ръководството на детската градина и ОИС.
    - Реакция при инциденти на със сигурността на информацията – при наличие на инциденти със сигурността на информацията се реагира в съответствие с документираните процедури.

12. Взаимоотношения с доставчици

12.1 Сигурност на информацията при отношения с доставчици – осигурена е защита на активите на детската градина, които са достъпни за доставчика.

- Сигурността на информацията при взаимоотношения с доставчици - с доставчика са договорени и документирани изисквания за сигурност на информацията, които намаляват рисковете, свързани с достъпа на доставчика до активите на детската градина .
- Разглеждане на сигурността в рамките на споразумения (примерен документ е анекс към договор за услуги) с доставчици - всички приложими изисквания към сигурността на информацията са въведени и потвърдени писмено от всеки доставчик, който може да има достъп, да обработва, да съхранява, да

разпространява или да предоставя ИТ инфраструктурни компоненти за информацията на детската градина .

- Верига за доставки на информационни и комуникационни технологии - споразуменията с доставчиците включват изисквания, отнасящи се за рисковете за сигурността на информацията, свързани с веригата за доставки на услуги и продукти на информационни и комуникационни технологии.

12.2 Управление на предоставянето на услуги от доставчици – поддържа се договореното ниво на сигурност на информацията и предоставянето на услуги в съответствие със споразуменията с доставчици.

- Наблюдение и преглед на услуги, предоставяни от доставчици - редовно се наблюдават, преглеждат и одитират предоставяните услуги от доставчиците.
- Управление на измененията на услугите, предоставяни от доставчици - измененията на предоставянето на услуги от доставчици, съдържащи поддържане и усъвършенстване на съществуващи политики, процедури и механизми за контрол за сигурност на информацията, трябва да бъдат управлявани, като се отчита критичността на информацията, системите и процесите, свързани с дейността и повторно оценяване на рисковете.

13. Обучение и повишаване на осведомеността

С цел поддържане на високо ниво на информационна сигурност, следва да се провеждане на редовни обучения за персонала, включително теми като разпознаване на фишинг атаки и създаване на силни пароли.

13.1 Обучение съгласно целевата аудитория

Участниците се разделят в групи, за да се насочи обучението според техните роли и отговорности:

- **Учители**: Как да защитават учебните материали и данните на децата.
- **Административен персонал**: Управление на чувствителни данни и реакция при инциденти.
- **Технически персонал**: Напреднали мерки за защита на мрежите и системите.

13.2 Основни теми за обучение

1. **Основи на информационната сигурност**:
   - Значение на информационната сигурност за детската градина.
   - Видове заплахи (фишинг, зловреден софтуер, неоторизиран достъп).
2. **Създаване на сигурни пароли**:
   - Използване на сложни пароли (12+ символа, включващи букви, цифри и специални символи).
   - Промяна на пароли на всеки 90 дни.
3. **Разпознаване на фишинг атаки**:
   - Примери за подозрителни имейли.
   - Действия при получаване на подозрителни съобщения (не кликвайте върху линкове, докладвайте инцидента).
4. **Защита на устройства**:
   - Актуализиране на софтуера и операционните системи.
   - Инсталиране на антивирусен софтуер.

- Неизползване на публични Wi-Fi мрежи без защита.

5. **Защита на данни**:
   - Принципи на минималния достъп („необходимост да знае“).
   - Криптиране на чувствителна информация.
6. **Реакция при инциденти**:
   - Как да се докладва инцидент на отговорното лице.
   - Стъпки за ограничаване на щетите.

13.3 **Формат на обучението**

- **Присъствени лекции**: Провеждане на сесии с примери и демонстрации.
- **Онлайн платформи**: Достъп до курсове или интерактивни обучения.
- **Симулации**: Практически упражнения, като например симулация на фишинг атака или тест за реакция при инцидент.

13.4 **Ресурси за обучение**

- **Материали**:
  - Презентации, наръчници и инфографики.
  - Примерни политики за информационна сигурност.
- **Инструменти**:
  - Онлайн тестове за проверка на знанията.
  - Видеа с обучителни сценарии.
- **Шаблони**:
  - Процедури за докладване на инциденти.
  - Контролни листи за защита на устройства и данни.

13.**5. Оценка на ефективността**

- Провеждат се тестове след обучението, за да оцените нивото на разбиране.
- Използват се казуси и сценарии за оценка на практическите умения.
- Редовно се преглежда програмата и актуализирайте съдържанието ѝ според новите заплахи и технологии.

13.6 **Периодичност на обучението**

- **Основно обучение**: В началото на учебната година за всички групи.
- **Допълнителни сесии**: На всеки шест месеца за нови заплахи или актуализации на политиките.
- **Обучение за нови служители**: Незабавно, при постъпване на работа

14. Съхранение и архивиране

14.1 Резервирането на информация трябва да бъдат направени и редовно изпитвани резервни копия на информация, софтуер и образи на системите.

14.2 Организацията трябва да има система за резервиране, която да прави веднъж седмично архив на всяко едно работно място. Архивът трябва да може да осигурява цялостно възстановяване на работното място включително възстановяване и на операционната система. Препоръчително е използване на автоматизирани системи за архивиране на всички критични данни и съхранение на архиви в криптиран вид на (отделна) физическа локация или в облачна услуга.

14.3 Следва да се разработи процес за редовно тестване на дейностите за възстановяване на данни.

15. Оценка на риска

15.1 Подход към оценката на риска

Оценката на риска представлява систематичен процес за идентифициране, анализ и управление на заплахите, които могат да засегнат информационната сигурност на детската градина.

- Идентификация на рисковете: Определят се всички потенциални заплахи за информационните активи, включително човешки грешки, технически неизправности, природни бедствия и злонамерени действия.
- Оценка на вероятността: За всяка заплаха се оценява вероятността тя да се реализира.
- Анализ на въздействието: Определя се какви биха били последствията при реализиране на заплахата (например загуба на данни, финансова загуба, репутационни щети).
- Оценка на съществуващите мерки: Проверява се ефективността на настоящите мерки за сигурност.

15.2 Процедура за управление на риска

- Провеждане на оценка на риска поне веднъж годишно.
- Изготвяне на доклад с резултатите и препоръки за подобрения.
- Приоритизиране на рисковете според тяхната критичност.
- Разработване и изпълнение на план за действие за намаляване на идентифицираните рискове.

15.3 Инструменти и отговорности

- Използват се специализирани инструменти за оценка на риска (напр. списъци за проверка, матрици за анализ на риска).
- Оценката се извършва от екип, включващ представители на ръководството, IT специалисти и учители.
- Примерна матрица за оценка на риска – Приложение №2

16. Съответствие

16.1Съответствие със законови и договорни изисквания – цели се пълно съответствие с нормативни или договорни задължения, отнасящи се към сигурността на информацията, както и на всички изисквания за сигурност.

- Защита на записите – записите са защитени от изгубване, изтриване, разрушаване, фалшифициране, неоторизиран достъп или неоторизирано огласяване в съответствие със законовите, нормативните и договорните изисквания и изисквания за дейността.

16.2 Тайна и защита на информацията за самоличността – осигурена е тайната и защита на информацията за самоличността според изискванията на съответните нормативни актове и регламенти, където са приложими.

16.3 Регламентиране на криптографски механизми за контрол – криптографски механизми за контрол и защита трябва да се използва в съответствие с всички приложими споразумения, нормативни актове и регламенти.

17. Одити и прегледи

17.1 Цели на одитите

- Да се провери дали политиката за информационна сигурност се прилага ефективно.
- Да се установят слабости в системата за сигурност и да се предложат коректривни действия.
- Да се гарантира съответствие с нормативната уредба и стандартите за сигурност.

17.2 Вътрешни одити

Провеждат се на тримесечие от назначен вътрешен екип.

Одитът обхваща:

- Правилата за достъп до информационни системи.
- Актуалността на защитния софтуер.
- Наличието и коректността на архивираните данни.

Докладите от вътрешните одити се представят на ръководството на детската градина и съдържат препоръки за подобрения на процеси, оптимизация на начин на работа и/или нужда от инвестиции за повишаване на нивото на физическа и техническа сигурност.

17.3 Външни одити (опционално)

Провеждат се от сертифицирани външни експерти поне веднъж годишно.
Основният фокус е върху съответствието с GDPR, Закона за защита на личните данни и други релевантни стандарти.
В случай на липса на външен одит, се изготвя вътрешна оценка на състоянието на контролите свързани с информационна сигурност и защита на личните данни, като същата се провежда от служител информационна сигурност, длъжностно лице за защита на данните и директор на детската градина.

17.4 Преглед на политиката

Политиката за информационна сигурност се преразглежда ежегодно.

Прегледът включва:

- Оценка на промените в технологичната среда и законодателството.
- Анализ на резултатите от одитите и инцидентите, ако има такива.

- Консултация с персонала за установяване на практически трудности в прилагането на политиката.

17.5 Документация и съхранение на резултатите

Всички документи от одити и прегледи се съхраняват в защитена среда за минимум 5 години.
Отговорникът по информационна сигурност поддържа централен регистър на одитите и тяхното изпълнение.

18. Спазване на политиката

Нарушенията на политиката водят до дисциплинарни мерки, като отнемане на права за достъп, административни действие (предупреждения и други), както и при необходимост – правни действия.

19. Обобщение
Политиката за информационна сигурност е основа за ефективното управление на данните и технологиите в детската градина. Всички страни трябва да са запознати и да се придържат стриктно към нея, съгласно своите роли, за да осигурят безопасна и надеждна среда.

Директор ДГ №40 „Проф. д-р Г. Ангушев“

Веселина Георгиева П

Приложение №1 – Регистър на активите

Приложение №2 – Матрица за оценка на риска

Приложение №3 – Заповед за въвеждане на политиките

Приложение №4 – Политика за защита и управление на личните данни