ДЕТСКА ГРАДИНА № 68 "Ран Босилек" – София,
Люлин VII, ул. "Ив. и Ст. Параскевови №5" ,тел. 02/825-72-40 , 02/925-01-67,
e-mail : odz68@abv.bg, www.dg68-ranbosilek.com

Политика за мрежова и информационна сигурност

1. Цел

Настоящата политика определя общия ред, отговорностите и минималните мерки за защита на мрежовите и информационните системи на детската градина. Документът служи като основа за всички по-подробни вътрешни правила, процедури, регистри и проверки.

2. Правно основание

Правната рамка, върху която е структуриран пакетът, включва Закона за киберсигурност (обн., ДВ, бр. 94 от 2018 г.; посл. изм. и доп., ДВ, бр. 17 от 13.02.2026 г.) и Наредбата за минималните изисквания за мрежова и информационна сигурност, приета с ПМС № 186 от 19.07.2019 г. (обн., ДВ, бр. 59 от 26.07.2019 г.).

Политиката е съобразена с изискването да се поддържа вътрешна политика по мрежова и информационна сигурност, която се преразглежда най-малко веднъж годишно и при съществена промяна в средата. При изготвянето са отчетени и насоките на европейската рамка по Директива (ЕС) 2022/2555 (NIS2), доколкото са относими към националната уредба и към добрите практики за организационни и технически мерки.

3. Обхват

Политиката се прилага за всички информационни системи, крайни устройства, мрежово оборудване, сървъри, безжични точки за достъп, облачни услуги, системи за видеонаблюдение, електронни дневници, служебни акаунти и бази данни, които се използват от училището.

Политиката обхваща и данните за ученици, родители, служители, контрагенти и документооборота, доколкото тези данни се обработват чрез горепосочените системи.

Политиката е задължителна за всички служители, външни изпълнители и други лица, на които е предоставен достъп до мрежата, системите, помещенията или данните на училището.

4. Основни цели

• запазване на поверителността, цялостта и наличността на информацията;

• осигуряване на непрекъсваемост на критичните процеси на детската градина;

• намаляване на риска от инциденти и ограничаване на въздействието им;

• ясно разпределяне на отговорностите между ръководството, определеното лице и външните изпълнители;

• поддържане на доказуемо съответствие чрез актуални документи, регистри, обучения и проверки.

5. Основни принципи

• мерките се определят според риска, мащаба на детската градина и реалните й процеси;

ДЕТСКА ГРАДИНА № 68 "Ран Босилек" – София,
Люлин VII, ул. "Ив. и Ст. Параскевови №5" ,тел. 02/825-72-40 , 02/925-01-67,
e-mail : odz68@abv.bg, www.dg68-ranbosilek.com

• предоставя се само минимално необходимият достъп до системи, данни и помещения;

• ползват се поддържани и актуални технологии, които могат да се управляват и проверяват;

• действията по администриране, промени и инциденти се документират, когато това е необходимо за сигурността и доказването;

• при възлагане на дейности на външни изпълнители ръководството запазва контрола и изисква проследимост.

6. Управление и отговорности

Директорът утвърждава политиката, осигурява организационни условия и ресурс за прилагането ѝ и провежда периодичен управленски преглед.

Определеното лице по мрежова и информационна сигурност координира прилагането на политиката, поддържа регистрите, следи за актуализацията на документите и приема и ескалира сигнали за инциденти.

Администраторите и външните изпълнители изпълняват конкретни технически задачи в рамките на предоставените им правомощия, без да заобикалят вътрешния ред и без да използват неразрешени общи акаунти.

Всички служители са длъжни да спазват вътрешните правила, да пазят поверените им устройства и акаунти и да уведомяват незабавно при съмнение за инцидент, загуба на устройство или неправомерен достъп.

7. Политика за мрежова инфраструктура

Мрежовата инфраструктура на детската градина включва кабелна и безжична мрежа, рутери, защитни устройства, суичове, точки за достъп, комуникационни шкафове, свързаните към мрежата сървъри, системи за архивиране и системи за видеонаблюдение, когато са интегрирани към средата на детската градина.

• физическата и логическата свързаност се описват и поддържат актуални, така че да е ясно кои устройства са критични и как са свързани;

• ключовите мрежови устройства се инвентаризират, обозначават и се пазят архиви на конфигурациите им по защитен ред;

• административната мрежа, учебната среда, безжичният достъп за служители, достъпът за гости и свързаните системи с по-висок риск се разделят, когато това е технически възможно и разумно;

• на мрежовите устройства се използват персонални административни профили или друг проследим ред; фабричните пароли и ненужните услуги се премахват или забраняват;

• отдалечено администриране се допуска само по одобрен защитен канал, с удостоверяване, журнал и ограничаване до упълномощени лица;

• актуализациите на фърмуер, критичните корекции и промените по конфигурацията се извършват по планиран ред и се документират;

ДЕТСКА ГРАДИНА № 68 "Ран Босилек" – София,
Люлин VII, ул. "Ив. и Ст. Параскевови №5" ,тел. 02/825-72-40 , 02/925-01-67,
e-mail : odz68@abv.bg, www.dg68-ranbosilek.com

• безжичните мрежи се защитават с подходяща автентикация и криптиране, а нерегламентираните точки за достъп не се допускат;

• комуникационните шкафове, patch панели, DVR и NVR устройствата и други критични точки се разполагат така, че физическият достъп до тях да е ограничен и проследим.

8. Минимален набор от организационни и технически мерки

• опис и периодичен преглед на активите, профилите и правата за достъп;

• анализ и оценка на риска и приоритизиране на мерките;

• архивиране и периодично тестване на възстановяването;

• вътрешен ред за приемане, регистриране и ескалация на инциденти;

• контрол върху доставчици, отдалечен достъп и договорни изисквания за сигурност;

• периодично обучение и инструктаж на персонала;

• годишни проверки, вътрешен одит и управленски преглед.

9. Преглед и актуализация

Политиката се преразглежда минимум веднъж годишно, както и при съществена промяна в инфраструктурата, системите, доставчиците, процесите, резултатите от оценката на риска или при значим инцидент.

При всяка актуализация следва да се провери дали са необходими промени и в останалите документи от пакета, включително вътрешните правила, процедурите, регистрите и плана за обучение.

10. Заключителна разпоредба

Настоящата политика влиза в сила от датата на утвърждаването ѝ със заповед на директора и е задължителна в рамките на определения обхват.

Утвърждавам:.....

Директор:.....

Дата:.15.09.2026г.

