ДЕТСКА ГРАДИНА № 163 – СО РАЙОН „ОВЧА КУПЕЛ”
гр. София – 1618, кв., бул. „Никола Петков” №141, тел.: 0882901671
nail: detska_gradina_163@abv.bg; info-2200058@edu.mon.bg; www.detskagradina

УТВЪРЖДАВАМ: П
СТЕФКА ШАТЕВА
ДИРЕКТОР НА ДГ № 163
Със заповед № 685-41/02.10.2026 г.
В сила от 02.10.2026 г.

ПОЛИТИКА

ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ДЕТСКА ГРАДИНА № 163

РАЗДЕЛ ПЪРВИ
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящата политика цели да регламентира: правила и процедури за използване на информационните системи и активи на Детска градина № 163 от страна на служителите:

1. запазване на конфиденциалността на информацията чрез осигуряване на мерки за защита от неправомерно придобиване, неправомерно модифициране, унищожаване или загубване;

2. развитие и поддържане на сигурни и надеждни информационни системи, осигуряващи цялост и достъпност на информацията;

3. мерки за реакция в случай на злоупотреба, загуба или неупълномощено придобиване на информация, както и при бедствия, и аварии;

4. осигуряване на непрекъснатост на работните процеси;

5. информиране на педагогическия и непедагогическия персонал и на други лица, имащи достъп до информационните системи и активи на ДГ № 163 за техните отговорности и задължения;

(2) Политиката обхваща:

1. **информационните системи на ДГ № 163;**
2. **информацията, съдържаща се в системите;**
3. **потребителите на информацията.**

(3) Политиката на ДГ № 163 не налага ограничения, противоречащи на установената култура на откритост и доверие в институцията.

(4) Целта на описаните в политиката контроли е да защитават служителите на ДГ № 164, потребителите, децата, както и външните заинтересовани страни, имащи отношения с институцията, от незаконни и увреждащи действия, извършени предумишлено или несъзнателно.

Чл. 2. Информационните системи и активи включват:

1. **информацията, създавана и използвана от ДГ № 163;**
2. **бази данни;**
3. **компютри, мобилни устройства, комуникационни устройства, устройства за копиране и всякакви периферни устройства;**
4. **WEB базирани и други информационни системи и софтуерни активи (програми), в това число операционни системи, вътрешна и интернет страница, имейли и др.;**
5. **локална мрежа и инфраструктура (окабеляване, захранване и др.);**
6. **носители на информация (дискови масиви, дискове, USB памети и др.).**

Чл. 3. При управление на сигурността на информацията, ДГ № 163 прилага стандарт БДС EN ISO/IEC 27001 – Информационни технологии – Методи за сигурност – Системи за управление на сигурността на информацията – Изисквания.

РАЗДЕЛ ВТОРИ
ОТГОВОРНОСТИ

Чл. 4. В ДГ № 163 се прилага и спазва принципът на разпределение на задълженията и отговорностите като средство за намаляване на риска от случайна или умишлена злоупотреба с информационните системи и активи.

Чл. 5. (1) Директорът на ДГ № 163:

1. **утвърждава настоящата политика и свързаните с нея документи, както и промените в тях;**
2. **разпределя правата за използване на информационните системи и ролите и отговорностите, свързани с опазване на информационните активи и сигурността на информацията;**
3. **координира прилагането на мерки за осигуряване на информационна сигурност;**
4. **оценява потребностите и планира необходимите ресурси за осигуряване на информационната сигурност;**
5. **утвърждава план за осигуряване непрекъснатостта на дейността и планове за обучение на служителите на ДГ № 163, във връзка с използването на информационните системи и активи и информационната сигурност.**

(2) Директорът на ДГ № 163 проследява и осигурява актуалността на настоящата политика и свързаните с нея документи.

(3) Директорът на ДГ № 163 отговаря за подходящото оповестяване на актуалната версия на настоящата политика и свързаните с нея документи. Той отговаря служителите на ДГ № 163 да бъдат подходящо инструктирани и мотивирани за изпълнение изискванията на политиката.

Чл. 6. Специалистът по информационни технологии/системният администратор отговаря за:

1. **управление и поддържане на информационните системи и активи на ДГ № 163 и предоставяне на нужните нива на достъп;**
2. **архивиране на данни и информация;**
3. **осигуряване на защита от злонамерен софтуер;**
4. **мониторинг на уязвимости и инциденти;**
5. **изготвяне на нужната документация, свързана с администрирането на информационната система и активи.**

Чл. 7. (1) Потребителите на информационните системи в ДГ № 163 са задължени да следват правилата, инструкциите и заповедите, свързани с използването на информационни системи и активи и с информационната сигурност.

(2) Потребителите са длъжни да докладват за проблеми и инциденти с информационните системи и активи.

(3) Под потребители на информационни системи в настоящата политика се разбират всички лица, които имат достъп до системите по силата на своите

служебни или договорни отношения.

(4) Педагогическите специалисти и непедагогическият персонал използват информационните системи и активи в ДГ № 163 с цел увеличаване на продуктивността и ефективността на работата.

(5) Всички потребители се запознават с тези части от настоящата политика и свързаните с нея документи, които отговарят на техните роли и отговорности. Потребителите потвърждават, че са запознати и че разбират задълженията си по тези документи.

(6) Правата и задълженията на потребителите и служителите на ДГ № 163 по отношение на информационните системи и активи и информационната сигурност в ДГ № 163, се определят в съответствие с настоящата политика, в правила, заповеди или в длъжностните им характеристики.

РАЗДЕЛ ТРЕТИ

ИНФОРМАЦИОННА СИГУРНОСТ И ЧОВЕШКИ РЕСУРСИ

Чл. 8. Директорът на ДГ № 163 отговаря за прекратяването или промяната на правата и достъпа до информационните системи и активи на служители или лица, с които ДГ № 163 е сключила договор и на които трудово-правните отношения или договорът се прекратява или променя.

Чл. 9. При необходимост, е възможно правата и достъпът до информационните системи и активи на служители, лица, с които ДГ № 163 е сключила договор да се продължат и за определен период след края на договора/напускане на образователната институция. В този случай лицето подписва декларация за конфиденциалност.

Чл. 10. При напускане на специалиста по информационни технологии или при прекратяване на договора с него, знанията за информационните системи и активи и за информационната сигурност на ДГ № 163 се документират по подходящ начин и се предават на образователната институция.

РАЗДЕЛ ЧЕТВЪРТИ

ИЗПОЛЗВАНЕ И УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ И АКТИВИ

Чл. 11. (1) Информационните системи и активи на ДГ № 163, в това число вътрешната мрежа от устройства, интернет, операционните системи, приложният софтуер и други, описани в чл. 2 на настоящата политика, са собственост на ДГ № 163.

(2) Данните и информацията, които служителите и потребителите обработват и съхраняват при изпълнение на служебните си задължения или в рамките на образователния процес чрез използване на информационните системи на ДГ № 163, са собственост на образователната институция.

(3) Информационните системи и активи на ДГ № 163 са предназначени да се използват единствено за постигане на целите и в интерес на образователната институция.

(4) ДГ № 163 поддържа пълен списък на информационните си системи и активи.

Чл. 12. (1) Работниците/служителите в ДГ № 163 нямат право да вземат програмни продукти с цел инсталацията им на домашните им компютри и преносими устройства, с изключение на електронни познавателни книжки и създадените за он-лайн обучение софтуери.

(2) Изключения от разпоредбата на ал. 1 са допустими при изрично разрешение на директора на ДГ № 163 и за целите на работния или образователния процес.

Чл. 13. При напускане на институцията, работниците/служителите нямат право да копират или унищожават файлове с данни, които са създадени във връзка с тяхната работа.

Чл. 14. (1) Забранява се ползването на информационните системи и активи на ДГ № 163 в следните случаи:

1. **Заобикаляне на системите за сигурност, с цел разрушаване или намаляване сигурността на учебната локална мрежа или бази данни.**
2. **Ползване на информационните системи за извършване на престъпление.**
3. **За подпомагане дейността на частни лица, в това число търговски дружества, техните продукти, услуги или бизнес практика.**
4. **Електронната поща на институцията не може да се ползва за комерсиални лични цели, религиозни цели или да се подпомага бизнес, който не е свързан с дейността на ДГ № 163.**
5. **За политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат.**
6. **Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност. Всички електронни писма, пращани от персонала трябва да са лично подписани.**
7. **Свалянето от интернет на аудио и видео файлове с нерагламентиран произход.**
8. **Сваляне и инсталиране на компютърни програми от интернет без разрешение на системен администратор.**
9. **Копиране на лицензираните компютърни програми на институцията с цел лична употреба.**

(2) Този списък на забранените дейности във връзка с информационните технологии не е изчерпателен и към него може да се добавят допълнителни забрани със заповед на директора.

Чл. 15. (1) Неоторизираното разкриване на служебна информация може да доведе до негативни последици за ДГ № 163 и накърняване на нейния имидж и репутация.

(2) Работник/служител, който е копирал и използвал информация от локалната мрежа на ДГ № 163 за лична изгода или за да причини вреда на институцията, носи съответната дисциплинарна и имуществена отговорност по

Кодекса на труда.

Чл. 16. (1) Директорът на ДГ № 163 насърчава ползването на интернет от работниците/служителите за обмяна на информация, извършване на проучвания и събиране на данни във връзка с дейността им.

(2) Директорът на ДГ № 163 отговаря за уместната употреба на интернет от персонала.

Чл. 17. Всички електронни писма и важни съобщения, които имат отношение към дейността на ДГ № 163, трябва да се принтират и представят за завеждане с входящ номер в Дневника за входяща кореспонденция от определеното длъжностно лице, като екземпляр се съхранява в съответния класьор и в електронната поща.

РАЗДЕЛ ПЕТИ

КОНТРОЛ ВЪРХУ РАБОТАТА С ИНФОРМАЦИОННИТЕ СИСТЕМИ И АКТИВИ

Чл. 18. (1) Директорът на ДГ № 163 има право да контролира ползването на програмните продукти, електронната поща, интернет и базите данни, създадени от педагогическите специалисти и непедагогическия персонал в образователната институция.

(2) Директорът на ДГ № 163 има право да проверява изцяло служебните компютри, предоставени за образователни цели на персонала в институцията, както и техниката, която ползват учители и служители във връзка с изпълнение на служебните им задължения.

(3) Служителите и потребителите са наясно, че работата и използването на информационните системи и активи подлежи на непрекъснато наблюдение.

(4) ДГ № 163 има право да деинсталира всякакъв софтуер или файлове, които не са свързани със служебните задължения на потребителя или с образователния процес, като (но не само) игри, музикални файлове, изображения, видеоклипове, споделени и безплатни програми, и др.

(5) Служителите и потребителите, имащи достъп до информационните системи, спазват политика за чисто бюро, чист екран и защита на ненадзиравани устройства.

(6) Служителите и потребителите прилагат изключително внимание при работа с информационните системи, в това число работа в интернет и работа с електронна поща, за да се предпазят от вируси, троянски коне и друг злонамерен софтуер.

Чл. 19. Резултатите от извършения контрол върху работата с информационните системи и активи на ДГ № 163 се считат за конфиденциални и не се разгласяват от ръководството.

РАЗДЕЛ ШЕСТИ

ЗАЩИТА НА ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ

Чл. 20. (1) При придобиване на софтуерни продукти, за целите на ДГ № 163, се гарантира, че са налице ясни договорни клаузи относно правата за интелектуалната им собственост;

(2) При разработване на нови или промяна на съществуващи софтуерни продукти за целите на ДГ № 163, в договорите за разработка се включват ясни клаузи, гарантиращи, че правата за интелектуалната собственост остават за

институцията;

РАЗДЕЛ СЕДМИ

ФИЗИЧЕСКА СИГУРНОСТ

Чл. 21. Информационните системи и оборудването на ДГ № 163, в това число копирни машини, факсове и мрежови принтери, се защитават физически от заплахи за сигурността и влияние на рискове от околната среда, с цел предотвратяване на загуби, щети или излагане на риск на активи и затрудняване или прекратяване на дейността на институцията.

Чл. 22. Помещенията, в които е разположено оборудване, свързано с информационните системи на ДГ № 163, се обособяват като защитени физически зони, с ограничен и контролиран достъп.

За целта директорът на ДГ № 163 издава заповед със съответните мерки и отговорни лица. Подобни мерки могат да включват секретни ключалки, дневник за достъп, видео наблюдение и др.

Мерките за физическа защита не трябва да възпрепятстват и затрудняват служебния и образователния процес.

Чл. 23. Изнасянето извън сградата на ДГ № 163 на информационни активи принадлежащи на институцията се извършва с разрешение от директора.

Чл. 24. Служебна информация не се оставя без надзор или контрол, което означава видима на екран.

Чл. 25. Физическият достъп на външни лица до информационните системи и активи на ДГ № 163 се извършва от и/или в присъствие на служители на образователната институция.

РАЗДЕЛ ОСМИ

КОНТРОЛ НА ДОСТЪПА, УПРАВЛЕНИЕ НА ИНЦИДЕНТИ И ЗАЩИТА ОТ ЗЛОНАМЕРЕН СОФТУЕР

Чл. 26. (1) Достъпът до информационните системи и активи на ДГ № 163 е индивидуален и се осъществява на база персонален потребителски профил.

(2) Персоналният потребителски профил съдържа следните данни:

1. **лични данни;**
2. **потребителско име и парола;**
3. **права за достъп.**

Чл. 27. (1) Паролите следва да съдържат малки и големи букви, цифри и специални символи, дължината им трябва да е не по-малко от 8 символа за потребителските и 12 символа за администраторските профили.

(2) Паролите на потребителските профили трябва да се сменят регулярно на период не по-голям от шест месеца.

(3) Паролите на административните профили трябва да се сменят регулярно на период не по-голям от три месеца.

(4) Потребителите трябва да пазят своите лични пароли в тайна.

Чл. 28. Правата за достъп са две основни групи – потребителски и административни. Администраторски права на достъп се определят със заповед на директора на институцията.

Чл. 29. При настройка на информационните системи на ДГ № 163 се

препоръчва да се прилага следният подход:

1. **след 5 (пет) неуспешни опита за влизане в системата, съответният профил се „заключва“. Отключването на профила се извършва от администратора, след изясняване на причините за заключването.**
2. **определя се максималното време на сесия без активност от страна на потребителя, след което профилът автоматично излиза от системата.**

Чл. 30. (1) Информационните системи и активи на ДГ № 163 трябва да бъдат надеждно защитени от проникване на злонамерен код (напр. вируси), хакерски атаки и др. Подобно проникване може да се осъществи както през Интернет, така и от неправилно използване на преносими информационни носители (дискове, външна памет и др.).

(2) Специалистът по информационни технологии на ДГ № 163 отговаря за поддържане на системите за защита от злонамерен код. За целта се използват като минимум:

1. **системи за защита;**
2. **софтуер за откриване на вируси, сканиращ както входящия трафик към външни (интернет) страници и платформи на институцията, така и към потребителските персонални компютри използвани в институцията.**

Чл. 31. (1) Специалистът по информационни технологии на ДГ № 163 носи пълната отговорност за избирането и инсталирането на антивирусната програма, както и за нейната актуализация на всеки индивидуален компютър. Служителите също трябва да следят дали тяхната антивирусна програма се осъвременява периодично с най-новата версия.

(2) Потребителите на информационните системи на ДГ № 163 трябва да приемат всяко съобщение за злонамерен софтуер или друго злонамерено събитие изключително сериозно и да следват вътрешните процедури за реакция в такъв случай.

(3) Преднамереното разпространяване на данни, за които потребителят знае, че са заразени с вирус е нарушение на служебните задължения, което се санкционира по дисциплинарен ред.

(4) В случай на злонамерена атака потребителят трябва незабавно да информира специалиста по информационни технологии, без да предприема никакви действия самостоятелно.

(5) Входящата електронна поща трябва да се третира с особено внимание поради потенциалната възможност да е заразена със злонамерен софтуер. Отварянето на приложения да се прави само след предварителното им сканиране с антивирусна програма.

(6) Ползването на външни носители (дискове, външна памет и др.) на информация е допустимо само след предварителното им сканиране с антивирусна програма.

Чл. 32. (1) ДГ № 163 събира и анализира данни за вида и броя на инцидентите, свързани със сигурността на информацията. Въз основа на анализа се прави преценка на разходите за защита. Също така, въз основа на анализа се идентифицират повтарящи се инциденти или инцидентите с голямо влияние и на тази база се оптимизират мерките за защита.

(2) Информацията от извършваните по предходната алинея анализи се взема предвид в процеса по управление на риска в ДГ № 163.

Чл. 164. При работа от разстояние и необходимост от достъп до

информационните системи на ДГ № 163 дистанционно – извън вътрешната мрежа:

1. **се използват само канали с висока степен на защита като Virtual Private Network (VPN);**
2. **не се използват File Transfer Protocol (FTP) и Remote Desktop Connection.**

РАЗДЕЛ ДЕВЕТИ

ПОДДЪРЖАНЕ НА ПЪЛНОТАТА, ИНТЕГРИТЕТА И КОНФИДЕНЦИАЛНОСТТА НА ИНФОРМАЦИЯТА

Чл. 34. (1) Основна отговорност за достоверността, актуалността и пълнотата на информацията, носят служителите, които имат право да я създават и записват в информационните системи на ДГ № 163.

(2) Промени във вече записана в информационните системи информация правят служителите, на които са дадени съответните права за това.

(3) В случай, че вече записана в информационните системи информация е затворена за редактиране през стандартния потребителски интерфейс, промените се извършват само след писмено разрешение на директора на ДГ № 163 и след като специалистът по информационните технологии „отключи“ възможността за редактиране.

(4) Конфиденциалността на информацията е лична отговорност на всеки, чийто профил осигурява достъп до нея, в съответствие с предоставените му права.

РАЗДЕЛ ДЕСЕТИ

АРХИВИРАНЕ И ВЪЗСТАНОВЯВАНЕ НА ИНФОРМАЦИЯТА

Чл. 35. (1) Сривовете в компютърното оборудване, вирусите и случайното изтриване на файлове могат да причинят загуба на данни, поради което е необходимо информацията във всяка компютърна система да бъде архивирана.

(2) Целта на архивирането е да се възстанови работата възможно най-бързо в случай на прекъсване по технически причини. По този начин се минимизират възможните проблеми и загуби.

(3) Специалистът по информационни технологии в ДГ № 163 осигурява на потребителите адекватна система за архивиране на данните от тяхната работа на подходящи технически носители (външни хард дискове, USB и др.).

(4) Честотата на архивирането се определя от директора в писмена процедура и зависи от броя транзакции и тяхната значимост за системата.

(5) Задължително архив (архивиране на файлове) се прави веднъж месечно.

Чл. 36. (1) Направените архивни копия се съхраняват по възможност извън основната сграда на ДГ № 163, в защитено помещение.

(2) Архивните копия се обозначават със следните данни:

1. **име на информацията;**
2. **дата на създаване;**
3. **срок на съхранение;**
4. **име на служителя, извършил архивирането.**

(3) Архивните копия се проверяват периодично за пълнота на архивираната информация и възможност за възпроизвеждането ù. Копията се проверяват поне веднъж годишно, а носители с информация от ключово значение за дейността на образователната институция – поне веднъж на 6 месеца.

Чл. 37. (1) При срив в информационните системи, специалистът по

информационни технологии предприема нужните действия за възстановяване на нормалното функциониране на системите.

(2) При загуба или повреждане на информация, специалистът по информационни технологии я възстановява, като използва последното актуално архивно копие.

РАЗДЕЛ ЕДИНАДЕСЕТИ

РАЗРАБОТВАНЕ И ВНЕДРЯВАНЕ НА ИНФОРМАЦИОННИ СИСТЕМИ

Чл. 38. С цел предотвратяване на увреждане или загуба на информация или грешки в информационните системи на ДГ № 163, при разработени и внедряване на нови или при усъвършенстване на съществуващи информационни системи, се планират подходящи мерки, които се залагат в договорите с разработчиците.

Чл. 39. (1) За всяка информационна система се поддържат отделни една от друга среда за тестване и продукционна среда, в която системата функционира.

(2) Дейности по разработване не се извършват в тестовата и продукционна среда на системата.

(3) Не се допуска пряк достъп на разработчиците до продукционната среда.

РАЗДЕЛ ДВАНАДЕСЕТИ

ОЦЕНКА НА РИСКА

Чл. 40. (1) Като част от дейността по управление на риска, ДГ № 163 идентифицира и оценява рисковете, свързани с използването на информационните системи и информационната сигурност.

(2) При оценката на риска се идентифицират рискове за всяка система и актив, описани в списъка по чл. 11, ал. 4 на настоящата политика.

(3) Въз основа от резултатите от оценката на риска, се прецизират и предприемат конкретните мерки, във връзка с областите на прилагане и защита на информационните технологии и информацията, описани в настоящата политика.

ДОПЪЛНИТЕЛНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящата политика се преглежда и при необходимост се актуализира поне веднъж годишно, при промени в приложимата уредба, в средата и технологиите, в организацията и дейността на ДГ № 163, а също така в резултат от промяна в рисковете, застрашаващи дейността на институцията.

§ 2. Директорът на ДГ № 163 създава условия за запознаването на служителите на образователната институция и всички потребители на информационните ù системи и активи с политиката, като публикува и комуникира политиката чрез подходящи комуникационни канали и организира обучения.

§ 3. Директорът на ДГ № 163 или определено от него лице упражнява контрол по прилагане на политиката.