Детска градина № 125 “Усмивка”

✉ п.к.1618 гр.София, р-н:“ Овча купел“, ул. “Монтевидео ” № 21А,
☎ тел.02/4261128 0884171459 0884801674
e-mail: usmivkadet@abv.bg

X

Albena Alipieva-Gerova
direktor

Утвърдил:
Директор:А.Алипиева - Герова

ПОЛИТИКА ЗА МРЕЖОВА И ИИНФОРМАЦИОННА СИГУРНОСТ НА

Приет на ПС по протокол№01/20.09.2022г. и утвърден със заповед №.566-40/20.09.2022г.

I. ОБЩИ ПОЛОЖЕНИЯ.

1. Цел, обхват и потребители

Целта на този документ е да се определят ясни правила за използването на информационната система и други информационни активи в Детска градина №125 „Усмивка“, София (за краткост ДГ).

Потребители на настоящата Политика са всички служители на ДГ.

2. Нормативна уредба

Стандарт ISO/IEC 27001

Наредба за минималните изисквания за мрежова и информационна сигурност.

II. ОСНОВНИ ПРАВИЛА ЗА СИГУРНОСТ НА ИНФОРМАЦИЯТА.

1. Определения:

Информационна система – включва всички работни станции, мрежова инфраструктура, системен и приложен софтуер, данни и други компютърни подсистеми и компоненти, които са собственост или се използват от ДГ или са под отговорността на ДГ. Използването на информационна система включва също и използването на всички вътрешни или външни услуги, като интернет достъп, електронна поща и др.

Информационни активи – в контекста на тази политика терминът *информационни активи* се прилага към информационните системи и към друга информация/оборудване, включително мобилни телефони, преносими компютри, носители за съхранение на данни и т. н.

Риск за сигурността на информационната система – възможността дадена заплаха да използва уязвимостта на актив или група активи и по този начин да причини вреда на организацията.

Ограничено разпространение – получателят може да споделя тази информация с други хора от организацията, но само ако е спазен принципът „необходимост да се знае“.

Вътрешно ползване – информацията в тази категория може да бъде разпространяване широко в рамките на дадена общност/организация, без да бъде изнасяна извън общността и без да бъде публикувана и поствана в интернет.

2. Приемлива употреба.

Информационните активи могат да се използват само за дейности, насочени към изпълнение на основните задачи на ДГ.

3. Отговорност за активите.

Всеки информационен актив има собственик, определен в инвентарния списък на активите. Собственикът на активите е отговорен за конфиденциалността, целостта и наличието на информация във въпросния актив.

4. Забранени дейности.

Забранява се използването на информационни активи по начин, по който ненужно се придобиват права, отслабва се работата на информационната система или представлява заплаха за сигурността. Забранява се също така:

4.1 да се изтеглят изображения или видео файлове, които нямат отношение към целите на ДГ, да се играят игри и т. н.;

4.2 да се инсталира софтуер на компютрите без изричното разрешение от Служителя по мрежова и информационна сигурност (СМИС) в ДГ;

изтегляне на програмен код от външни носители;

4.3 да се инсталират или използват периферни устройства, като например модеми, карти с памет или други устройства за съхраняване и четене на данни (например USB флаш устройства) без изрично разрешение от СМИС.

5. Изнасяне на активи извън ДГ.

Оборудване, информация или софтуер, независимо от неговата форма или носител, не могат да бъдат взети извън района на ДГ без предварително писмено разрешение от СМИС. Докато тези активи са извън ДГ, те трябва да бъдат контролирани от лицето, което е получило разрешение за изнасянето им.

6. Връщане на активите при прекратяване на трудовия договор.

При прекратяване на трудов договор или друг договор, въз основа на който се използва различно оборудване, софтуер или информация в електронен или хартиен вид, потребителят трябва да върне всички такива информационни активи на СМИС.

7. Процедура за архивиране.

На потребителя трябва да се архивира всяка чувствителна информация, съхранена на неговия компютър, най-малко веднъж на ден.

8. Антивирусна защита.

Антивирусен софтуер трябва да се инсталира на всеки компютър с активирани автоматични актуализации.

9. Разрешителни за използване на информационната система.

Ползвателите на информационната система могат да имат достъп само до активите на информационната система, за които са изрично упълномощени от собственика на актива.

Ползвателите могат да използват информационната система само за целите, за които са получили разрешение, т. е. за които са получили права на достъп.

Потребителите не трябва да участват в дейности, които могат да се използват за заобикаляне на контролите за сигурност на информационните системи.

10 Отговорности на потребителския акаунт.

Потребителят не трябва, пряко или косвено, да позволи на друго лице да използва неговите права на достъп, т. е. потребителско име, и не трябва да използва потребителското име и/или паролата на друго лице. Забранено е използването на потребителски имена на групи.

Собственикът на потребителския акаунт е неговият потребител, който е отговорен за използването му и всички транзакции, извършвани чрез този потребителски акаунт.

11. Правила за паролите.

Потребителят трябва прилага добри практики за сигурност по отношение на пароли:

11.1 паролите не трябва да се разкриват пред други лица, включително управленски персонал и системни администратори;

11.2 паролите не трябва да се записват, освен ако конкретен защитен метод не е одобрен от СМИС;

11.3 потребителски генерирани пароли не трябва да се разпространяват чрез комуникационни канали (чрез устно, писмено или електронно разпространение и т. н.);

11.4 паролите трябва да се променят при индикации, че те или системата може да са били компрометирани – в този случай трябва да бъде отчетен инцидент със сигурността;

11.5 трябва да се изберат силни пароли по следния начин:

- използване на най-малко осем символа
- използване на поне един цифров знак
- използване на поне една главна буква и поне един малък буквен знак
- паролата не трябва да бъде дума от речник, диалект или жаргонна дума
- паролите не трябва да се основават на лични данни (напр. дата на раждане, адрес, име на член на семейството и т. н.)
- последните три пароли не трябва да се използват повторно

11.6 паролите трябва да се сменят на всеки 3 месеца;

11.7 паролите, използвани за лични цели, не трябва да се използват за бизнес цели.

12. Използване на интернет.

Интернет може да бъде достъпен на работните станции в ДГ само чрез нейната локална мрежа, с подходяща инфраструктура и защита на защитната стена.

ДГ може да блокира достъпа до някои интернет страници за отделни потребители, за групи от потребители или за всички служители и ученици в ДГ. Ако достъпът до някои уеб страници е блокиран, потребителят може да подаде писмено искане до СМИС за разрешение за достъп до такива страници. Потребителят не трябва да се опитва да заобиколи такова ограничение автономно.

Потребителят трябва да счита за ненадеждна информацията, получена чрез непотвърдени уеб сайтове. Тази информация може да се използва само след проверка на нейната автентичност и коректност.

Потребителят е отговорен за всички възможни последици, произтичащи от неоторизирано или неподходящо използване на интернет услуги или съдържание.

13. Имейл и други методи за обмен на съобщения.

Методи за обмен на съобщения, различни от електронна поща, включват изтегляне на файлове от интернет, трансфер на данни чрез факс апарати, изпращане на SMS текстови съобщения, форуми и социални мрежи.

СМИС определя комуникационния канал, който може да се използва за всеки тип данни, както и възможните ограничения за това кой има право да използва комуникационните канали, т. е. определя кои дейности са забранени.

Потребителите могат да изпращат само съобщения, съдържащи вярна информация. Забранено е да се изпращат материали с обезпокоителни, неприятни, явно сексуално, груби, клеветнически или всякакви други неприемливи или с незаконно съдържание. Потребителите не трябва да изпращат спам съобщения на лица, с които не е установена делова връзка или на лица, които не са изисквали такава информация.

Потребителят трябва да запише всяко съобщение, което съдържа данни, значими за дейността на ДГ, като използва метода, зададен от СМИС.

Ако даден потребител публикува съобщение на система за обмен на съобщения (социални мрежи, форуми и т. н.), той/тя трябва недвусмислено да заяви, че не представлява гледна точка на ДГ.

14. Авторското право.

Потребителите не трябва да правят неоторизирани копия на софтуер, собственост на ДГ, освен в случаите, разрешени от закона, от собственика или от СМИС.

Потребителите не трябва да копират софтуер или други оригинални материали от други източници и са отговорни за всички последици, които биха могли да възникнат съгласно Закона за интелектуалната собственост.

III. УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА.

1. Организиране на дейностите по управление на сигурността на информацията.

Управлението на сигурността на информацията в ДГ се осъществява от неговото ръководство, което:

1.1 разработва ясни разпоредби и проявява постоянна ангажираност по въпроса;

1.2 определя Служител по мрежова и информационна сигурност, който да координира дейностите и контролира спазването на изискванията за сигурност на информацията;

1.3 изрично определя отговорностите на всеки служител по отношение на сигурността на информацията, информира служителя за тези отговорности чрез неговото запознаване и подписване на Декларация за спазване на изискванията по мрежова и информационна сигурност и организира обучение на служителите в изпълнение на задълженията им по мрежова и информационна сигурност.

1.4 поддържа контакти с компетентните местни и държавни органи за осигуряване на физическата сигурност на сградата на ДГ, с повишено внимание на опазването на информационните активи.

1.5 организира преглед на дейностите по управление на сигурността на информацията през планирани интервали или при настъпили съществени промени в дейността на ДГ, но не по-рядко от веднъж в рамките на една календарна година.

2. Управление на ресурси:

2.1 Управление на човешките ресурси.

Управлението на човешките ресурси, в т.ч. изискванията за сигурност, са регламентирани в съответна Политика на ДГ.

За служителите, които се явяват нарушители на политиките и процедурите по сигурността на информацията, особено при причиняване на щети на ДГ, се предприема официален дисциплинарен процес съгласно вътрешните правила и националното законодателство, в т.ч и с помощта на юридически консултанти.

2.2 Управление на технологичните ресурси:

2.2.1 опис на информационните активи.

СМИС, съвместно със системния администратор, изготвят опис на информационните активи на ДГ. В описа са включени всички важни за ДГ информационни активи, като за всеки актив са посочени неговият собственик и местоположение. Описът се поддържа на хартиен носител и в електронна форма и се актуализира при настъпили промени в активите (добавяне на нов актив, преоценка на актив, бракуване на актив и др.). На активите се извършва оценка на риска по групи по реда на утвърдената методология. Воденето на регистър на активите не отменя задължението да се спазват всички изисквания за инвентаризация и управление на материалните средства в съответствие със счетоводните изисквания и политиката на администратора.

2.2.2 използването на информация и активи, свързани със средства за обработване на информацията, е позволено само за служебни цели и в рамките на конкретни служебни правомощия.

2.2.3 финансово-счетоводната документация и документацията, свързана с управление на персонала, се обработва, съхранява и идентифицира съгласно приложимите нормативни изисквания. Обработването се осъществява на работни станции с персонализиран достъп, разположени в помещения с ограничен достъп.

2.2.4 информационни активи, които подлежат на бракуване и унищожаване, се съхраняват временно в помещение в склад на ДГ. След решение на ръководството те се предават на външна фирма, лицензирана за управление на този вид отпадък, и се унищожават по сигурен и позволен начин.

2.2.5 закупуването и въвеждането в експлоатация на нови средства за обработване на информацията се извършва след одобрение от ръководството, от оценени доставчици. Процесът на одобрение протича в следната последователност:

- предложение за въвеждане (закупуване) на средство за обработване на информация;
- съгласуване на предложението със системния администратор по отношение на съвместимост, капацитет, производителност, условия за поддръжка, начин на обслужване, средства за контрол;
- съгласуване на предложението със СМИС по отношение на изискванията за информационна сигурност;
- одобряване на средството за обработване на информация от Директора на ДГ или от упълномощено лице;
- въвеждане в експлоатация с извършване на приемателни тестове на средството за обработване на информация;
- определяне на отговорник на средството за обработване на информация, което е актив за ДГ;
- въвеждане на корекции в документацията, ако това е необходимо. Извършва се от СМИС и Длъжностното лице по защита на данните (ДЛЗД).

3. Контрол на достъпа:

3.1 Достъп на потребителите на информационната система.

В ДГ се упражнява физически и логически контрол за достъп на потребителите до информационните ресурси. Паролите се съставят съгласно добрите практики за избор на пароли и се подновяват регулярно.

Правата за достъп на потребителите се преглеждат поне веднъж годишно, а също и при възникнала необходимост, от СМИС и системния администратор, които изготвят писмен доклад за резултатите от прегледа.

3.2 Достъп на трети страни.

Преди предоставянето на достъп до ресурси на ДГ на трети страни, въпросите, свързани със сигурността на информацията, се разглеждат от СМИС и ДЛЗД, които дават писмено становище. Договорите, включващи достъп и обработване на информация на ДГ

или добавяне на продукти и услуги към средствата за обработване на информацията, съдържат изисквания за сигурност. Същите се преглеждат от ръководството преди предоставяне за подпис от физическото или юридическото лице и впоследствие при преглед на изпълнението на договора.

Преди предоставяне на достъп до ресурси на ДГ на трети страни, съответните лица подлежат на предварително проучване от страна на СМИС и ДЛЗД (попадат ли в списъка с лицата, упълномощени да извършват договорената дейност, дали са надеждни и очаквано лоялни доставчици, референции и препоръки за извършването на подобни дейности и др.).

Водят се записи за всяко посещение, физическо вмешателство, извършена услуга или осъществен контакт, свързан с обмен на информация или приемо-предаване на устройства или софтуер.

Изискванията за поверителност и неразкриване на тайна, отразяващи потребностите на ДГ от защита на информацията, са определени в декларации за конфиденциалност и клаузи в договорите. Всички договори с трети страни съдържат клауза, предвиждаща санкции и съдебни действия при неизпълнение на договорените условия за конфиденциалност.

4. Физическа сигурност и сигурност на заобикалящата среда.

ДГ е в сгради с масивни конструкции. Входната врата през деня е контролирана от физическа охрана.

Осъществява се видеонаблюдение на прилежащия на външната фасада район и площадката пред входната врата със средства на Столична община.

Компютрите, комуникационната и офис техника се разполагат в служебните помещения върху офис мебели, така че да бъдат предпазени от неблагоприятни въздействия.

ДГ при необходимост предприема мерки за дублиране на комуникационното оборудване и преносната среда чрез алтернативно оборудване, канали и доставчици.

Прилагат се правила, които регламентират процесите при поддръжка и предоставяне на външни контрагенти за ремонт устройства, съхраняващи информация. Целта е да се предотврати неконтролирано изнасяне на информация извън ДГ.

ДГ прилага политика за „чисто бюро” и „чист екран”. На лицата, обработващи лични данни, се забранява оставянето без надзор на преносими памети или други носители на информация, включително с лични данни. Забранява се оставянето без надзор на бюрата и масите в работните помещения на документи, бележки или данни, записани или съхранени в хартиена или електронна форма, представляващи потенциална заплаха за сигурността на информацията.

Забранено е използването на самозалепващи се листа за водене на бележки върху екраните на използваните от тях работни станции с информация за пароли. Неспазването на тази точка се счита за дисциплинарно нарушение и се наказва съгласно вътрешните

правила на ДГ. Скрийнсейвърите на компютрите са настроени да се заключват автоматично на 15 минути без действие от страна на служителите, които нямат право да променят тази настойка.

5. Сигурност на операциите.

СМИС и системният администратор целенасочено събират информация за новини, статистики, изследвания, инциденти, тенденции и прогнози в областта на зловредния софтуер. Събраните материали се използват за актуализация на документацията и обучение на служителите по отношение на сигурността на информацията.

За предпазване от злонамерен код се използват антивирусни програми, които се обновяват автоматично. Устройствата се сканират регулярно. Извършват се проверки (периодични или при наличие на конкретен повод) на оригиналния софтуер (Integrity checks) на всички критични за дейността на ДГ информационни системи. При констатиране на несъответствия (отсъствие на файлове, наличие на допълнителни файлове, променени файлове) те се разследват с цел изясняване на причините и оценка на последиците.

Всеки случай на проникване или на съмнение за проникване на зловреден код се докладва незабавно на СМИС и се изпълняват дадените от него указания.

Резервираненето и архивирането на информацията се извършва автоматично и ръчно в процеса на оперативната работа, като се спазват утвърдените правила и процедури. В случаи, когато срокът за съхранение на информацията е по-дълъг от жизнения цикъл на носителя, се предвижда своевременно прехвърляне на друг носител. Отговорност за това действие носят собственикът на актива (носителя на информация) и СМИС.

Не се допуска използване на лични информационни носители за служебни цели. Не се допуска съхранение на служебна информация на лични информационни носители. Задължение на всеки отговорник на актив и служител е да съхранява информационните носители по начин, който е препоръчан от съответния производител, и осигурява тяхната цялост и достъпност за оторизираните лица.

Съхраняването на документацията на информационните системите се осигурява от СМИС.

Изисква се наличие на контролен механизъм за управление и проследимост на инциденти и ясен срок за докладването им, което налага предварителна подготвка на инфраструктурата.

Поддържат се средства за осигуряване на валидни в съда доказателства за целите на евентуално разследване и търсене на наказателна отговорност за умишлено престъпно нарушение на политиките и процедурите по защита на информацията и на личните данни и причиняване на щети на ДГ. При необходимост от официални наказателни мерки срещу нарушители на сигурността на информацията, същите се инициират и провеждат от ръководството, като при необходимост се ползват и външни юридически услуги.

6. Сигурност на средствата за обработване и обмен на информация.

Средствата за обработване на информация, собственост на ДГ, периодично се подлагат на преглед с цел навременно идентифициране на евентуални проблеми в тяхното функциониране и откриване на недостатъци в тяхната защита.

6.1 на преглед и анализ подлежат:

6.1.1 оторизираният достъп на потребители, в това число:

- идентификаторите на потребителите;
- дата и час на настъпили събития;
- вид на настъпилите събития;
- файлове, с които е работено;
- използвани програми и помощни средства.

Целта е да се осигури проследимост на използването на информационните системи от потребителите.

6.1.2 действия с информационните системи, при които са ползвани привилегии:

- използване на привилегировани акаунти (от системни администратори);
- стартиране и спиране на информационна система;
- включване/изключване на входно/изходни устройства.

Целта е да се осигури проследимост на опитите за достъп и промяна на информационната система от привилегировани потребители.

6.1.3 установяване на неоторизирани опити за достъп, в това число:

- неуспешни или отхвърлени действия на потребители;
- неуспешни или отхвърлени действия по отношение на масиви от данни или други ресурси;
- нарушение на политиката за достъп;

Целта е да се осигури своевременно разкриване и предотвратяване на нелегитимни опити за достъп и ползване на ресурсите на информационната система.

6.1.4 промени или опити за промяна на настройки и механизми за контрол на сигурността на система.

Целта е своевременно да бъдат разкривани и предотвратявани евентуални опити за манипулиране на защитата на информационната система с произтичащите от това последици за нейната сигурност.

6.2 честотата на прегледите на информационните системи зависи от:

- значението на конкретната информационна система за дейността на ДГ;
- характера на обработваната информация;
- наличие на досегашни опити за пробив в сигурността на информационната система;
- степен на обвързаност на системата.

6.3 Системният администратор извършва периодичните прегледи на информационните системи, обобщава резултатите от тях и ги използва за докладване на евентуални инциденти по информационната сигурност и защита на личните данни и при подготовката на материали по искане на контролните органи.

IV. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ СЪС СИГУРНОСТТА НА ИНФОРМАЦИЯТА.

Всеки служител на ДГ, на когото станат известни слабости или инциденти, свързани със сигурността на информацията или съмнения за такива слабости, е длъжен незабавно да ги докладва по електронна поща и по телефон на ръководството на ДГ и СМИС.

ДГ осигурява регистрация, проследимост и отчетност на докладите чрез записването им в съответния Регистър на нарушенията на сигурността, където се посочват естеството на инцидента/проблема, дата и час на регистриране, предприети мерки, дата и час на отстраняване, отговорно лице и др.

Инцидент би могло да предизвика проникване на зловреден код в системите, който да доведе до злоупотреба или загуба на информация, неоторизиран достъп до електронния дневник, загубване или повреждане на счетоводна документация, повреждане на важни документи в електронния архив и др.

Събития по сигурността, които задължително се докладват на СМИС и ДЛЗД:

- повреди в информационна система и загуба на услуга;
- установяване на злонамерен код;
- грешки в работата на системите или устройствата;
- загуба или повреда на хартиени документи, файлове, архиви;
- установени нарушения на политиките и процедурите за сигурност на информацията;
- съмнително поведение на доставчик или служител и др.;
- установена загуба на лични данни, неоторизиран достъп и злоупотреба с лични данни;

Регистрираните събития се проверяват от СМИС и ДЛЗД, които изготвят доклади до Ръководството на ДГ.

ДГ обменя със своите контрагенти информация за евентуални наблюдавани от тях слабости в сигурността на информацията с цел предприемане на своевременни мерки за недопускане на инциденти.

ЗАПОЗНАТИ СЛУЖИТЕЛИ В ДГ №125»УСМИВКА» с **ПОЛИТИКА ЗА МРЕЖОВА И ИИНФОРМАЦИОННА СИГУРНОСТ**

№	Име ,презиме и фамилия	длъжност	подпис
