ДЕТСКА ГРАДИНА № 98 „СЛЪНЧЕВОТО ЗАЙЧЕ”

гр. София, ж – к „Младост” -2, ул. „Слънчево зайче”№ 9

тел.: 02/ 885 37 32, odz98director@abv.bg www.odz98bg.com

ПРИЛОЖЕНИЕ КЪМ ЗАПОВЕД № 139 / 03.02..2021 г.

УТВЪРДИЛ:

Жанин Ценова

Директор на ДГ № 98 „Слънчевото зайче“

ВЪТРЕШНИ ПРАВИЛА

ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

НА

ДЕТСКА ГРАДИНА № 98 „СЛЪНЧЕВОТО ЗАЙЧЕ“

2021 г.

СЪДЪРЖАНИЕ

1. РАЗДЕЛ I: ЦЕЛ ……3
2. РАЗДЕЛ II: ОСНОВНИ ПОЛОЖЕНИЯ ……3
3. РАЗДЕЛ III: МИНИМАЛНИ МЕРКИ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ……4
4. РАЗДЕЛ IV: ДОКУМЕНТИРАНА ИНФОРМАЦИЯ НА ИНФОРМАЦИОННИ АКТИВИ ……...5
5. РАЗДЕЛ V: ОЦЕНКА И УПРАВЛЕНИЕ НА РИСКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ……6
6. РАЗДЕЛ VI: УПРАВЛЕНИЕ НА ВЗАИМОДЕЙСТВИЯТА С ТРЕТИ СТРАНИ…….....10
7. РАЗДЕЛ VII: АДМИНИСТРИРАНЕ НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ……...11
8. РАЗДЕЛ VIII: УПРАВЛЕНИЕ НА ДОСТЪПА НА УЧАСТНИЦИТЕ В ЕЛЕКТРОННИЯ ОБМЕН……12
9. РАЗДЕЛ IX: ЗАЩИТА СРЕЩУ НЕЖЕЛАН СОФТУЕР ……...13
10. РАЗДЕЛ X: МОНИТОРИНГ НА СЪБИТИЯТА И ИНЦИДЕНТИТЕ В ИНФОРМАЦИОННИТЕ СИСТЕМИ НА ДГ № 98 „СЛЪНЧЕВОТО ЗАЙЧЕ.....14
11. РАЗДЕЛ XI: ФИЗИЧЕСКА СИГУРНОСТ …….....15
12. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ …….....15
13. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ …….....16
14. ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ…….....16
15. ПРИЛОЖЕНИЯ……..17

РАЗДЕЛ I
ЦЕЛ

Чл. 1. Настоящият документ има за цел да регламентира вътрешните правила за мрежова и информационна сигурност на информационните системи на Детска градина № 98 „Слънчевото зайче“ в съответствие с ***Наредба за минималните изисквания за мрежова и информационна сигурност (НМИМИС)***, Обн., ДВ, бр. 59 от 26.07.2019 г., в сила от 26.11.2019 г., към ***Закон за киберсигурност,*** Обн., ДВ, бр. 94 от 13.11.2018г. и във връзка с изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО, наричани за краткост „Вътрешни правила“.

РАЗДЕЛ II
ОСНОВНИ ПОЛОЖЕНИЯ

Чл. 2. Вътрешните правила, указват правата и задълженията на потребителите на услугите, предоставяни чрез информационните и комуникационните системи на ДГ № 98 „Слънчевото зайче“, като използване на персонални компютри, достъп до ресурсите на корпоративната мрежа, генериране и съхранение на паролите, достъп до интернет, работа с електронна поща, системи за документооборот и други вътрешноведомствени системи, принтиране, факс, използване на сменяеми носители на информация в електронен вид, използване на преносими записващи устройства.

Чл.3. С цел гарантиране на информационната сигурност, ефективно и ефикасно използване на информационните системи потребителите са задължени да изпълняват настоящите вътрешни правила.

Чл. 4. Създаването, разместването или преконфигурирането на работни места в ДГ № 98 „Слънчевото зайче“, на чието разположение са или се предвижда да бъдат предоставени компютри се съгласува с директора на градината.

Чл. 5. Тези правила са приложими за всички служителите, които при изпълнение на служебните си задължения получават достъп до информационно-комуникационните ресурси (ИКР) на ДГ № 98 „Слънчевото зайче“.

РАЗДЕЛ III

МИНИМАЛНИ МЕРКИ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

Управление на мрежовата и информационната сигурност

Чл. 6. (1) Директора на детската градина определя със заповед Звеното за мрежова и информационна сигурност (ЗМИС), което отговаря за мрежовата и информационната сигурност при работа с ИКР.

(2) Административно звено по, ал. 1 е пряко подчинено на директора на детската градина.

(3) Звеното за мрежова и информационна сигурност осъществява следните функции:

1. Ръководи дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност, и целите, заложени в политиката на ДГ със звената за информационно осигуряване;

2. Участва в изготвянето на политиките за мрежова и информационна сигурност и документираната информация;

3. Следи за спазването на настоящите вътрешни правила и прилагането на законите, подзаконовите нормативни актове, международните стандарти, политиките и правилата за мрежовата и информационната сигурност;

4. Ръководи периодичните оценки на рисковете за мрежовата и информационната сигурност;

5. Периодично, но не по-малко от веднъж годишно, изготвя доклади за състоянието на мрежовата и информационната сигурност в административното звено и ги представя на директора на ДГ;

6. Планира и координира обученията, свързани с мрежовата и информационната сигурност;

7. Организира проверки за актуалността на плановете за справяне с инцидентите и плановете за действия в случай на аварии, природни бедствия или други форсмажорни обстоятелства като анализира резултатите от тях и организира изменение на плановете, при необходимост;

8. Поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност;

9. Следи за точното водене на регистъра на инцидентите;

10. Уведомява за инциденти съответния секторен екип за реагиране на инциденти с компютърната сигурност в съответствие с изискването на чл. 31, ал. 1 от НМИМИС;

11. Организира анализ на инцидентите с мрежовата и информационната сигурност за откриване на причините за тях и предприемане на мерки за отстраняването им с цел намаляване на еднотипните инциденти и намаляване на загубите от тях;

12. Следи за актуализиране на използвания софтуер;

13. Следи за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлага адекватни мерки за противодействието им;

14. Предлага за дисциплинарно наказание, служителите нарушили мерките за мрежова и информационна сигурност;

(4) За всяка от териториалните структури на ДГ, се определя служител от външна фирма, отговарящ за мрежовата и информационната сигурност.

РАЗДЕЛ IV
ДОКУМЕНТИРАНА ИНФОРМАЦИЯ НА ИНФОРМАЦИОННИ АКТИВИ

Чл. 7. (1) С цел намаляването на загуби от инциденти чрез скъсяване на времето за реагиране и разрешаването им, както и за намаляване на вероятността от възникване на инциденти, породени от човешки грешки, ДГ поддържа следната документация:

1. опис на информационните активи;

2. физическа схема на свързаност;

3. логическа схема на информационните потоци;

4. документация на структурната кабелна система;

5. техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти;

6. инструкции/вътрешни правила за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер;

7. вътрешни правила за служителите, указващи правата и задълженията им като потребители на услугите, предоставяни чрез информационните и комуникационните системи, като използване на персонални компютри, достъп до ресурсите на корпоративната мрежа, генериране и съхранение на паролите, достъп до интернет, работа с електронна поща, системи за документооборот и други вътрешноведомствени системи, принтиране, сканиране, факс, използване на сменяеми носители на информация в електронен вид и използване на преносими записващи устройства.

Чл. 8. (1) „Информационни активи" по смисъла на НМИМИС са информационните и комуникационните системи и обслужващата ги инфраструктура, в процесите и дейностите, в конфигурациите, в софтуера - материалните и нематериалните активи и информационни обекти, свързани с информационна система, които имат полезна стойност за ДГ.

(2) Информационните активи включват апаратурата, софтуера, данните, поддържащата инфраструктура и другите ресурси, свързани с мрежата и информационните системи в сградата на градината.

(3) За информационните ресурси се поддържат инвентарни списъци, определящи персоналната отговорност на всеки служител за зачислените му информационни ресурси (компютри, периферни устройства, софтуерни продукти и др.).

Чл. 9. За управление ДГ използва лицензирани софтуерни продукти.

Чл. 10. За комуникационната инфраструктура в сградата на ДГ се поддържа:

1. Опис на мрежовите устройства.
2. Схема на кабелните системи на ДГ.

Чл. 11. (1) При управлението и контрола на информационните активи се спазват следните правила:

1. Инсталират само софтуерни продукти, за които има придобито право за ползване (лиценз или др.).
2. Инсталирането и настройката на нов софтуер и хардуер се планира и се извършва в периоди с минимално натоварване на съответните ресурси;
3. Когато е приложимо, преди извършване на инсталация се правят резервни копия на софтуера, файловете и базите данни;

РАЗДЕЛ V
ОЦЕНКА И УПРАВЛЕНИЕ НА РИСКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

Чл. 12. Анализ и оценка на риска за мрежовата и информационната сигурност се извършва регулярно от ЗМИС, но не по-рядко от веднъж годишно, или когато се налагат съществени изменения в целите, вътрешните и външните условия на работа, информационната и комуникационната инфраструктура, дейностите или процесите.

Чл. 13. Оценката на риска за мрежова и информационна сигурност се дефинира чрез определяне на вероятността за уязвяване въз основа на ефективността на съществуващите или планираните мерки за сигурност.

Чл. 14. Заплахите за мрежовата и информационната сигурност се класифицират по следните критерии:

1. елементите на информационната сигурност (достъпност, цялостност, конфиденциалност), към които са насочени;

2. компонентите на информационната система (апаратура, софтуер, данни, поддържаща инфраструктура), към които са насочени;

3. начина на осъществяване (случайни/преднамерени действия, от природен/технологичен характер и др.);

4. разположението на източника (вътре в/извън информационната система).

Чл. 15. Действията по управление на риска за мрежова и информационна сигурност обхващат оценка на неговия размер, изработване на ефективни и икономични мерки за неговото снижаване и оценка дали резултативният риск е в приемливи граници. Управлението на риска се извършва чрез последователно прилагане на два типа циклично повтарящи се действия:

1. оценка (преоценка) на риска;

2. избор на ефективни и икономични средства за неговата неутрализация.

Чл. 16. При идентифициране на риск за мрежова и информационна сигурност се предприема едно от следните действия:

1. ликвидиране на риска (например чрез отстраняване на причиняващите го обстоятелства);

2. намаляване на риска (например чрез използване на допълнителни защитни средства);

3. приемане на риска и разработване на план за действия в обстановка на риск;

4. преадресиране на риска (например чрез сключване на съответната застраховка).

Чл.17. Процесът на управление на риска включва следните етапи:

1. избор на анализируемите обекти и нивото на детайлизация на анализа;

2. избор на методология за оценка на риска;

3. идентификация на информационните активи;

4. анализ на заплахите и последствията от тях, откриване на уязвимите места в защитата;

5. оценка на рисковете;

6. избор на защитни мерки;

7. реализация и проверка на избраните мерки;

8. оценка на остатъчния риск - явява се начало на нов цикъл на оценка, който се

провежда ако остатъчният риск не удовлетворява ръководството на администрацията. Оценка на остатъчния риск се извършва минимум веднъж в годината.

Чл. 18. Видовете заплахи срещу мрежовата и информационната сигурност, които могат да застрашат конфиденциалността, интегритета и достъпността, са следните:

1. Подслушване, изразяващо се в достъп до служебна информация чрез прихващане на електронни съобщения, независимо от използваната технология;
2. Електромагнитно излъчване, изразяващо се в действия на трето лице, целящо да получи знание за обменяни данни посредством информационна система;
3. Нежелан код, който може да доведе до загуба на конфиденциалността чрез записването и разкриването на пароли и до нарушаване на интегритета при интервенции от трети лица, осъществили нерегламентиран достъп с помощта на такъв код. Нежелан код може да се използва, за да се заобиколи проверка за достоверност, както и всички защитни функции, свързани с нея. В резултат кодът може да доведе до загуба на достъпността, когато данните или файловете са разрушени от лицето, получило нерегламентиран достъп с помощта на нежелан код;
4. Маскиране на потребителската идентичност може да доведе до заобикаляне на проверката за достоверност и всички услуги и защитни функции, свързани с нея;
5. Погрешно насочване или пренасочване на съобщенията може да доведе до загуба на конфиденциалност, ако се осъществи нерегламентиран достъп от трети лица. Погрешното насочване или пренасочване на съобщенията може да доведе и до нарушаване на интегритета, ако погрешно насочените съобщения са променени и след това насочени към първоначалния адресат. Погрешното насочване на съобщения води до загуба на достъпността до тези съобщения;
6. Софтуерни грешки могат да застрашат конфиденциалността, ако софтуерът е създаден с контрол на достъпа или за криптиране или ако грешка в софтуера осигури възможност за нежелан достъп в информационна система;
7. Кражбата на информационни активи може да доведе до разкриване на информация, която представлява служебна или друга защитена от закона тайна. Кражбата може да застраши достъпността до данните или информационното оборудване;
8. Нерегламентиран достъп до компютри, информационни ресурси, услуги и приложения може да доведе до разкриване на поверителни данни, на лични данни на физически лица и до нарушаване интегритета на тези данни, ако нерегламентираната им промяна е възможна. Нерегламентираният достъп до

компютри, данни, услуги и приложения може да наруши достъпността до данните, ако тяхното изтриване или заличаване е възможно;

9. Нерегламентиран достъп до носител на данни може да застраши съхраняваните върху него данни;
10. Повреждане на носител на информация може да наруши интегритета и достъпността до данните, които се съхраняват на този носител;
11. Не извършването на редовна поддръжка на информационните системи или допускане на грешки по време на процеса по поддръжка може да доведе до нарушаване на достъпността до данни;
12. Аварии в електрозахранване и климатични инсталации могат да доведат до нарушаване на интегритета и достъпността до данни, ако вследствие на настъпването на авариите са увредени информационни системи или носители на данни;
13. Технически аварии (например аварии в мрежите) могат да нарушат интегритета и достъпността до информация, която се съхранява или разпространява чрез тази мрежа;
14. Грешки при предаването на информацията могат да доведат до нарушаване на нейната цялост и достъпност;
15. Употреба на нерегламентирани програми и информация могат да нарушат интегритета и достъпността до данните, съхранявани и разпространявани чрез информационната система, в която е настъпило такова събитие, и програмите и информацията се използват, за да се изменят съществуващи програми и данни по неразрешен начин или ако те съдържат нежелан код;
16. Потребителски грешки могат да нарушат интегритета и достъпността до данни чрез неумишлено или умишлено действие;
17. Липса на потвърждаване може да застраши интегритета на данните. Предпазните мерки за предотвратяване на непотвърждаването трябва да се прилагат в случаите, когато е важно да се получи доказателство за това, че дадено съобщение е изпратено и е/не е получено, както и за това, че мрежата е пренесла съобщението;
18. Интервенции срещу интегритета на данните могат да доведат до тяхното сериозно увреждане и до невъзможност от по-нататъшното им използване;
19. Аварии в комуникационното оборудване и услуги могат да увредят достъпността на данните, предавана чрез тези услуги;
20. Външни въздействия с огън, вода, химикали и др. могат да доведат до увреждане

или унищожаване на информационното оборудване;

21. Злоупотреба с ресурси може да доведе до недостъпност до данни или услуги;

22. Природни бедствия могат да доведат до унищожаване на данни и информационни системи;

23. Претоварване на комуникационния трафик може да доведе до нарушаване на достъпността до обменяни данни.

РАЗДЕЛ VI

УПРАВЛЕНИЕ НА ВЗАИМОДЕЙСТВИЯТА С ТРЕТИ СТРАНИ

Чл. 19. (1) При установяване на взаимоотношения с трети страни, ДГ договаря изисквания за мрежова и информационна сигурност, включващи:

1. сигурност на информацията, свързана с достъпа на представители на трети страни до информация и активи на ДГ;

2. доказателства, че третата страна също прилага адекватни мерки за мрежова и информационна сигурност, включително клаузи, доказващи прилагането на тези мерки чрез документи и/или провеждане на одити;

3. прозрачност на веригата на доставките като третата страна трябва да е способна докаже произхода на предлагания ресурс/услуга и неговата сигурност;

4. последици при неспазване на изискванията за сигурност на информацията;

5. отговорност при неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за постигане на целите на мрежовата и информационната сигурност;

6. взаимодействие в случай на възникване на инцидент, който най-малко включва: контактни точки, начин за докладване, време за реакция, време за възстановяване на работата, условия за затваряне на инцидента.

РАЗДЕЛ VII

АДМИНИСТРИРАНЕ НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ

Чл.20. (1) ДГ № 98 „Слънчевото зайче“ прилага следните мерки за защита на профилите с

административни права за информационните и комуникационните системи и техните компоненти:

1. преди въвеждане в експлоатация задължително се сменят идентификационните данни на администратора, въведени по подразбиране или инсталирани от производителя/доставчика на информационния актив;

2. администраторските профили са персонални;

3. администраторските профили се използват само и единствено за административни цели;

4. администраторските профили се създават само на служители, които извършват административни операции (инсталиране, конфигуриране, управление, поддръжка и т. н.);

5. правата на всеки администраторски акаунт са ограничени във възможно най-голяма степен до функционалния и техническия периметър на всеки администратор;

6. данните за автентикацията на администраторските акаунти трябва да:

а) са различни за всяка система;

б) са с възможно най-голяма сложност, позволена от системата или нейния компонент;

7. веднъж годишно се прави преглед на администраторските профили с цел удостоверяване на актуалността им.

РАЗДЕЛ VIII
УПРАВЛЕНИЕ НА ДОСТЪПА НА УЧАСТНИЦИТЕ В ЕЛЕКТРОННИЯ ОБМЕН

Чл. 22. Потребители на компютърната и информационна среда на ДГ са всички служителите по трудово правоотношение.

Чл. 23. (1) Средствата за управление на достъпа позволяват да се определят и контролират действия, които различни-типове потребители на информационните системи и процеси в тях, могат да извършват по отношение на информационни ресурси.

(2) В зависимост от делегираните права и изпълняваните функции по отношение на вътрешните информационни и мрежови ресурси на ДГ, се дефинират следните типове потребители:

1. системни администратори;
2. администратори на потребителски акаунти;
3. администратори на информационни системи;
4. потребители с достъп до информационните ресурси с общо предназначение;
5. потребители с достъп до информационните ресурси със специализирано предназначение;

6. потребители с ограничен достъп до информационните ресурси.

Чл. 24. Новите потребители се запознават с настоящите Вътрешни правила при предоставяне на служебен акаунт за достъп до информационната инфраструктура на ДГ.

РАЗДЕЛ IX
ЗАЩИТА СРЕЩУ НЕЖЕЛАН СОФТУЕР

Чл. 25 Нежеланият софтуер, който може да експлоатира уязвимостта на един или няколко информационни актива и да предизвика смущаване на нормалната им работа, увреждане или унищожаване, включва някои от следните основни програми и атаки:

1. Malware - зловреден софтуер, предназначен да повреди, наруши функционирането, откраднe, разруши или като цяло да извърши негативни и нелегитимни действия в рамките на компютърни системи;
   - компютърни вируси;
   - мрежови червеи;
   - троянски коне;
   - логически бомби;
2. Ransomware - Рансъмуерът - криптира достъпа до дадена компютърна система или информация, като се изисква заплащането на откуп, за да премахне ограничението.;
3. Dos/DDos атаки- DDoS (Distributed Denial of Service) е разпространена атака за отказ (блокиране) на уебсайтове и имейл услуги. В този вид атака системата се бомбардира с толкова много пакети, че процесите се забавят или системата блокира.
4. Spam и Phishing атаки на имейл услуги - "Нежелана електронна поща".;
5. Други;

Чл. 26. За ефективна защита срещу нежелан софтуер в информационната инфраструктура на ДГ се изисква изпълнението на следните задължителни условия:

1. Използване само на регламентиран софтуер, в мрежата и на локалните компютри.

2. Задължително използване на антивирусен и антиспам софтуер.

3. Забранява се използване на програми извън обичайните и касаещи дейността на конкретния служител.

4. Забранява се използването на обслужващи програми, които могат да преодолеят механизмите за контрол на системите, както и активирането на злонамерени програми в компютърното оборудване (например: вируси, червеи, троянски коне, e-mail бомби и др. подобни).

Чл. 27. (1) При установяване на открити опити за проникване трябва незабавно да се предприемат следните действия:

1. да се уведоми директора за предприемане на адекватни мерки;
2. да се изключат или ограничат мрежовите услуги, свързани с актива - обект на проникването.
3. да се уведоми длъжностното лице по защита на личните данни.

Чл. 28. (1) **Забранено е** неоторизирано използване, чрез включване в USB портовете на компютърните системи на външни устройства, лични технически средства (зареждане на GSM-смарт телефони) и преносими записващи устройства (Flash памети, SSD дискове**)** и други.

(2) Всеки стационарен компютър, преносим компютър или мобилно устройство, което се включва в мрежата на ДГ, се проверява автоматично за вируси и нежелан софтуер, преди да получи достъп до ресурсите на мрежата.

Защита при отдалечен достъп/работа от разстояние

Чл. 29. При достъп до информационни активи извън мрежата, контролирана от ДГ, се спазват следните изисквания:

1. използва се най-малко двуфакторна автентикация;
2. използват се само канали с висока степен на защита като Virtual Private Network (VPN);
3. не се използват File Transfer Protocol (FTP) и Remote Desktop Connection.

РАЗДЕЛ X
МОНИТОРИНГ НА СЪБИТИЯТА И ИНЦИДЕНТИТЕ В ИНФОРМАЦИОННИТЕ СИСТЕМИ НА ДГ

Уведомяване за инциденти

Чл. 30. При настъпване на инциденти или събития свързани с пробиви в сигурността и заразяване с нежеланият софтуер, който може да експлоатира уязвимостта на един или няколко информационни актива и да предизвика смущаване на нормалната им работа, увреждане или унищожаване, служителите на ДГ, уведомяват незабавно директора на ДГ.

Чл. 31. Информацията за събития и инциденти, свързани с мрежата в ДГ се регистрират в

Регистър на събития и инциденти, свързани с информационната сигурност, по образец на Приложение № 2, който съдържа:

1. дата и време на настъпване на събитието;
2. описание на събитието;
3. резултат от събитието;
4. източник на събитието;
5. списък на засегнатите обекти;
6. предприети действия.

Чл. 32. ДГ организира анализ на инцидентите с мрежовата и информационната сигурност за откриване на причините за тях и предприемане на мерки за отстраняването им с цел намаляване на еднотипните инциденти и намаляване на загубите от тях.

РАЗДЕЛ XI
ФИЗИЧЕСКА СИГУРНОСТ

Чл. 33. За осигуряване на физическата защита на информационните системи ДГ предприема следните мерки:

1. мерки по управление на физическия достъп;
2. противопожарни мерки;
3. защита на поддържащата инфраструктура;
4. защита на мобилните системи.

Чл. 34. Допускането на външни посетители в ДГ и присъствието на служители в сградите извън определеното време, се извършва съобразно пропускателния режим в сградата на ДГ.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§ 1. По смисъла на тези правила:

1. „Информационни активи" са информационните и комуникационните системи и обслужващата ги инфраструктура, в процесите и дейностите, в конфигурациите, в софтуера или във фърмуера - материалните и нематериалните активи и информационни обекти, свързани с информационна система, които имат полезна стойност за ДГ

2. „Трети страни“ означава физически или юридически лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които

под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни.

3. Хардуерен срив – прекъсване или липса на информационни услуги в резултат на повреда на хардуерно устройство.

4. Софтуерен срив – прекъсване или липса на информационни услуги в резултат на активиране на софтуерни грешки или недостатъци.

5. Потребителски срив – прекъсване или липса на информационни услуги в резултат на умишлена или неволна намеса на потребител на системата.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Настоящите правила се утвърждават със заповед на директора на ДГ и влизат в сила от датата на утвърждаването им.

2. Правилата се актуализират при необходимост. Актуализацията на правилата се утвърждава от Директора на ДГ.

ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

НМИМИС	Наредба за минималните изисквания за мрежова и информационна сигурност
ДГ	Детска градина
ИТИСКО	Информационни технологии, информационни системи и комуникационно осигуряване
БД ИС	База данни Информационни системи
ИКР	Информационно-комуникационните ресурси
ЗЕУ	Закона за електронното управление
VPN	Виртуалната частна мрежа (VPN) разширява частна мрежа в обществена мрежа и позволява на потребителите да изпращат и получават данни в споделени или публични мрежи, сякаш техните изчислителни устройства са пряко свързани с частната мрежа.
Malware	Зловреден софтуер, предназначен да повреди, наруши функционирането, открадне, разруши или като цяло да извърши негативни и нелегитимни действия в рамките на компютърни системи.
Ransomware	Рансъмуерът - криптира достъпа до дадена компютърна система или информация, като се изисква заплащането на откуп, за да премахне ограничението.
Dos/DDos атаки-	DDoS (Distributed Denial of Service) е разпространена атака за отказ (блокиране) на уебсайтове и имейл услуги. В този вид атака системата се бомбардира с толкова много пакети, че процесите се забавят или системата блокира.
Spam и Phishing	"Нежелана електронна поща".;

Приложение № 1

ДЕКЛАРАЦИЯ

Долуподписаният/та .....

на длъжност.....

група .....

ДЕКЛАРИРАМ,

че съм запознат и ще спазвам „ВЪТРЕШНИ ПРАВИЛА за мрежова и информационна сигурност на ДГ", разработени в съответствие с Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност към Закона за електронно управление, приета с ПМС 279/17.11.2008г.

Като ползвател ДАВАМ СЪГЛАСИЕТО СИ за провеждане на мониторинг и протоколиране на управлението на достъпа ми в електронния обмен.

ДЕКЛАРИРАМ, че разбирам, приемам и ще изпълнявам изискванията за мрежова и информационна сигурност на информационните системи в ДГ, както и на конкретните документи от нейната рамка, адресирани към длъжността ми.

УВЕДОМЕН СЪМ, че при неспазване на изискванията за мрежова и информационна сигурност на информационните системи в ДГ, нося дисциплинарна и имуществена отговорност в съответствие с действащото законодателство.

Дата: ..... г. **ДЕКЛАРАТОР:**

Приложение № 2

РЕГИСТЪР НА СЪБИТИЯ И ИНЦИДЕНТИ, СВЪРЗАНИ С ИНФОРМАЦИОННАТА СИГУРНОСТ В ДГ № 98 „СЛЪНЧЕВОТО ЗАЙЧЕ“

Дата и време на настъпване на събитието	Описание на събитието	Резултат от събитието	Източник на събитието	Списък на засегнатите обекти	Предприети действия
1	2	3	4	5	6