ДЕТСКА ГРАДИНА № 127 „СЛЪНЦЕ“

гр. София 1408, р-н „Триадица“,

ул. „Деде Агач“ № 42

тел.: 02 958 92 91, e-mail: info-2224919@edu.mon.bg

УТВЪРЖДАВАМ: Т. БАКАЛОВА
/ ДИРЕКТОР /
ЗАПОВЕД № 88/15.09.2023 г.

Вътрешни правила за мрежова и информационна сигурност на ДГ № 127 „Слънце“

Приети на заседание на ПС от 15.09.2023 г.

I. ОБЩИ ПОЛОЖЕНИЯ

Чл.1. (1) Настоящите вътрешни правила определят политиката, организацията, управлението и контрола на киберсигурността и уреждат предприемане на необходимите мерки за постигане на високо общо ниво на мрежова и информационна сигурност в ДГ № 127 „Слънце“.

(2) Киберсигурност е състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им.

(3) Киберсигурността включва мрежова и информационна сигурност, противодействие на киберпрестъпността и киберотбрана.

(4) Мрежова и информационна сигурност е способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях.

(5) Мерките за мрежова и информационна сигурност са организационни, технологични и технически и се прилагат в съответствие със спецификата на ДГ № 127 „Слънце“ и пропорционално на заплахите с цел минимизиране на риска от тяхното реализиране.

(6) Мерките по ал. 5 гарантират основните цели на мрежовата и информационната сигурност, а именно запазване на достъпността, интегритета (цялост и наличност) и конфиденциалността на информацията по време на целия й жизнен цикъл (създаване, обработване, съхранение, пренасяне и унищожение) във и чрез информационните и комуникационните системи на Субекта.

(7) Мерките по ал. 5 са съобразени с изискванията на националните нормативни актове, регламентите на Европейския съюз и приетите и приложени от ДГ № 127 „Слънце“ стандарти, като се вземат предвид краткосрочните, основните и общите рискове за сигурността за съответния сектор.

(8) Мерките за мрежова и информационна сигурност се прилагат съобразно указанията на приложимите международни стандарти, посочени в приложение № 1 на Наредба за минималните изисквания за мрежова и информационна сигурност, препоръките на производители и доставчици на софтуер и хардуер, както и с добрите практики, препоръчани от водещи в областта на сигурността организации.

(9) Мерките по ал. 5 са:

1. Разнородни – постигането на всяка от целите на мрежовата и информационната сигурност се реализира с различни по характер и специфика мерки, което създава условие за многослойна защита, или т. нар. "дълбока отбрана";
2. Конкретни и лесни за възприемане, за да се гарантира, че мерките

действително се прилагат;

3. Ефикасни – да имат най-голямо въздействие върху потенциални заплахи, като се избягва ненужен разход на ресурси;

4. Пропорционални на рисковете – с оглед на постигане на оптимално съотношение между разходи и ползи при реализиране на целите на мрежовата и информационната сигурност;

5. Проверими – гарантират, че ДГ № 127 „Слънце“ може да предостави на съответния национален компетентен орган по смисъла на чл. 16 от Закона за киберсигурност доказателства за ефективното им прилагане в съответствие с изискването на чл. 16, ал. 3 от същия закон.

(10) В настоящите вътрешни правила понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми.

Чл.2. ДГ № 127 „Слънце“ поддържа система за управление на сигурността на информацията, която включва следните организационни мерки:

1. Разпределение на отговорностите за мрежовата и информационната сигурност;

2. Прилагане на политика за мрежовата и информационната сигурност;

II. РАЗПРЕДЕЛЕНИЕ НА ОТГОВОРНОСТИТЕ ЗА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ

Чл.3. Директорът на ДГ № 127 „Слънце“:

1. Носи пряка отговорност за мрежовата и информационната сигурност, дори и когато дейността е възложена за изпълнение на трети страни;

2. Създава условия за прилагане на комплексна система от мерки за управление на тази сигурност по смисъла на международен стандарт БДС ISO/IEC 27001; системата обхваща всички области на сигурност, които засягат мрежовата и информационната сигурност на ДГ № 127 „Слънце“, включително физическата сигурност на информационните и комуникационните системи;

3. Осигурява необходимите ресурси за прилагане на пропорционални и адекватни на рисковете организационни, технически и технологични мерки, гарантиращи високо ниво на мрежова и информационна сигурност в обхвата на наредбата;

4. Упражнява контрол върху нивото на мрежовата и информационната сигурност;

5. Определя, документира и налага отговорности по изпълнението, контрола и информираността за всички процеси и дейности, свързани с развитието, поддръжката и експлоатацията на информационните и комуникационните системи, като се спазва принципът, че едно лице не може да контролира

собствената си дейност.

6. Определя нивото на достъп до отделните системи и приложения на служителите и на външните лица в съответствие със задълженията им.

7. Организира регулярни обучения на служителите в ДГ № 127 „Слънце“ относно киберхигиена и добри практики за мрежова и информационна сигурност.

Чл.4. Със заповед на директора се определя служител или административно звено, отговарящо за мрежовата и информационната сигурност за всички териториални структури на ДГ №127 „Слънце“, като:

(1) Служителят или звеното, отговарящо за мрежовата и информационната сигурност, е на пряко подчинение на директора, с цел пряко информиране за състоянието и проблемите в мрежовата и информационната сигурност;

(2) Основни функции на служителя или на звеното, отговарящо за мрежовата и информационната сигурност:

1. Ръководи дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност, и целите, заложени в политиката на ДГ № 127 „Слънце“.

2. Участва в изготвянето на политиките и документираната информация.

3. Спазва вътрешните правила за мрежовата и информационната сигурност.

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

5. Веднъж годишно изготвя доклади за състоянието на мрежовата и информационната сигурност в звеното и ги представя на ръководителя.

6. Участва в 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. Анализира резултатите от тях и организира изменение на плановете, ако е необходимо.

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

9. Администрацията на ДГ № 127 “Слънце“ води регистър на инцидентите и уведомява за инциденти съответния секторен екип за реагиране на инциденти с компютърната сигурност в съответствие с изискването на чл. 31, ал. 1 (уведомяване за инциденти) от Наредбата за минималните изисквания за мрежова и информационна сигурност.

10. Администрацията 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.

11. Следи за актуализиране на използвания софтуер и фърмуер.

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

13. Сътрудничи на фирмата за поддръжка на ИКТ на ДГ № 127 „Слънце“ при

организиране и провеждане на тестове за откриване на уязвимости в информационните и комуникационните системи и изпълнява мерки за отстраняването им.

14. Организира и сътрудничи при провеждането на одити, проверки и анкети и при изпращането на резултатите от тях на съответния национален компетентен орган.

15. Подлежи на санкции при нарушаване на мерките за мрежовата и информационната сигурност.

16. Периодично да се извършва резервиране и архивиране на информацията.

Чл.5. Директорът на ДГ № 127 „Слънце“ подписва договори с външни организации за поддръжка на ИКТ и за доставчик на интернет услуги.

(1) Фирмата за поддръжка на ИКТ има следните отговорности:

1. Актуализира схемите на ИТ инфраструктурата и описа на информационните активи;
2. Отговарят за поддръжката и администрирането на системите, приложенията и мрежовите устройства и взимат мерки за защита от кибератаки.
3. Редовно проверяват дали антивирусните програми работят с актуални бази с данни от вирусни дефиниции.
4. Следят дали са приложени последните актуализации, отстраняващи уязвимости в сигурността на използваните софтуерни продукти, операционни системи и фърмуер на устройствата.
5. При необходимост прави тестове за уязвимости в мрежовата и информационната сигурност на ИК инфраструктурата, както и за уязвимости в сигурността на уеб сайта на ДГ № 127 „Слънце“.

(2) Фирмата доставчик на интернет услуги предприема контрамерки срещу кибератаки и ранното им откриване.

Чл.6. Служителите в ДГ № 127 „Слънце“ са длъжни да подадат сигнал до директора в случай на кибератака, а директорът от своя страна да уведоми Националния екип за реагиране при инциденти с компютърна сигурност, създаден към ДАЕУ на следните контактни точки: 02/949 22 12, 0878 908 546, cert@govCERT.bg

За инцидентите, които имат въздействие върху непрекъснатостта на дейността на ДГ № 127 „Слънце“ се докладва два пъти:

- Първоначално уведомяване, което се прави до два часа след констатирането на инцидента;
- В срок до 5 работни дни, като се предоставя пълната информация за инцидента.

  За целите на докладването следва да се използва Приложение № 7 /към чл. 31, ал. 2 от Наредбата за минималните изисквания за мрежова и информационна сигурност.

III. ПРИЛАГАНЕ НА ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

Чл.7. (1) Политиката за мрежова и информационна сигурност в ДГ № 127 „Слънце“ се преразглежда редовно, но не по-рядко от веднъж годишно и при необходимост се актуализира.

(2) Политиката има отношение към и включва всички съответни специфични политики за сигурност на информационните и комуникационните системи:

1. Забранява се на външни лица работата с персоналните компютри на ДГ № 127 „Слънце“, освен за :
   - упълномощени фирмени специалисти в случаите на първоначална инсталация на компютърната и периферна техника, програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място;
   - провеждане на обучения на външни педагогически специалисти по програми и проекти на МОН и РУО.
2. След края на работния ден всеки служител задължително изключва компютъра, на който работи;
3. Забраняват се опити за достъп до компютърна информация и база данни, до които не са предоставени права, съобразно заемана от служителя длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп;
4. Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства се извършва само след съгласуване с директора на ДГ № 127 „Слънце“;
5. Служителите имат право да обменят компютърна информация във връзка с изпълнение на служебните си задължения;
6. Достъпът до помещенията със сървърите за видеонаблюдение се ограничава само до специализиран по поддръжката им персонал;
7. Ползването на компютърна мрежа, електронни платформи, интернет и служебна електронна поща, комуникатори, осигуряващи достъп извън рамките на компютърната мрежа на ДГ № 127 „Слънце“ от служителите става чрез получените потребителско име и парола, като служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност за това;

(3) ДГ № 127 „Слънце“ поддържа информация, доказваща по неоспорим начин изпълнението на изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

(4) Информацията по ал. 3:

1. Се поддържа в актуално състояние;
2. Е достъпна само за:

а) тези лица, които е необходимо да я ползват при изпълнение на служебните си

задължения по силата на трудови, служебни или договорни отношения;
б) представители на съответните национални компетентни органи съгласно чл. 16, ал. 5 от Закона за киберсигурност;
в) други организации, оправомощени с нормативен акт или договорни отношения.

IV. КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

Чл. 8. (1) ДГ № 127 „Слънце“ в качеството си на администратор на лични данни извършва класификация на информацията, която определя как да се маркира, използва, обработва, обменя, съхранява и унищожава информацията, с която разполага.

(2) Класификацията по ал. 1 се прилага и върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето и унищожаването на информацията, като към тях трябва да се прилагат подходящи механизми за защита, съответстващи на идентифицираните заплахи.

(3) Всяка информация, която стане достъпна за служителите при изпълнение на служебните им задължения, ако са свързани с ДГ № 127 „Слънце“ и нейната дейност, родители или външни организации се счита за собствена и поверителна информация на детската градина, като по този начин се подчинява на защита в съответствие с приложимите закони и правната уредба, относно защитата на поверителна информация, търговската тайна и личните данни.

(4) Информацията подлежи на защита, независимо от това дали такава информация е на разположение на служителя под формата на печатни материали, устройства за съхранение на данни, аудио/видео материали или по друг начин.

(5) Обща класификация на информацията, приложима в рамките на ДГ № 127 „Слънце“:

Категория/Ниво/	Описание	Примери/неизчерпателни/
Публична информация/Ниво 0	Информация, която може да бъде обработвана и разпространявана в рамките на ДГ № 127 „Слънце“ или извън нея без никакво отрицателно въздействие върху детската градина, някои от нейните партньори, родители и/или свързани лица.	Цялата информация публикувана на уебсайта на ДГ № 127 „Слънце“, на родителските табла по групи.
Вътрешна информация/Ниво 1	Информацията в тази категория може да бъде разпространявана широко в рамките на дадена общност. Въпреки това информацията не може да бъде публикувана или поствана в интернет, както и изнасяна извън общността.	Вътрешна комуникационна мрежа на ниво администрация на ДГ № 127 „Слънце“ – всякакви документи свързани с дейността на детската градина; Информация публикувана в родителските вайбър групи от учителите в група – снимки на децата, видеоклипове,

		официални съобщения, документи за попълване и др.
Вътрешна информация/Ниво 2	Получателят може да споделя тази информация с други хора от детската градина, но само е спазен принципът „Необходимост да се знае“. Ако получателят на информацията иска да я разпространява, задължително трябва да се консултира с източника.	Цялостна документация на ДГ № 127 „Слънце“, работна кореспонденция, информация, получена чрез вътрешни вайбър групи, имейл кореспонденция и др.
Поверителна информация/Ниво 3	Информацията не се оповестява и разпространяването и е ограничено само до участниците, обработващи, съхраняващи или обменящи информацията. Разкриването на тази информация би могло да окаже неблагоприятно въздействие върху дейността, репутацията и цялостното състояние на ДГ №127 „Слънце“, родители, партньори и свързани лица, като последица от такова разкритие, която би причинила сериозни вреди/щети на някое от тези лица.	Лични данни, търговски тайни, финансова информация. Информация, която подлежи на защита по силата на споразумение за поверителност, което се подписва от дадения служител. Информация, която подлежи на защита по силата на споразумения за поверителност или споразумения за сътрудничество, които ДГ № 127 „Слънце“ е сключила в хода на дейността си.

V. ПЛАН ЗА ДЕЙСТВИЕ ПРИ ИНЦИДЕНТИ И В СЛУЧАЙ НА АТАКА

Чл.9. План за действие при инциденти и в случай на атака.

1. Отговорник за организацията при подобна ситуация – Директорът на ДГ № 127 „Слънце“;
2. Функционална и йерархична ескалация – служителят, открил пробива в сигурността веднага информира директора, директорът информира външната организация за поддръжка на ИКТ и Националния екип за реагиране при инциденти с компютърната сигурност;
3. Външната организация по поддръжката на ИКТ ще следи за всички параметри по време на атаката;
4. Събирането и съхраняването на необходимата информация ще се извършва от външната организация по поддръжката на ИКТ.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите Вътрешни правила за мрежова и информационна сигурност са разработени на база Закон за киберсигурност 2018 г., Наредба за минималните изисквания за мрежова и информационна сигурност 2019 г. и Указания за повишаване нивото на мрежовата и информационната сигурност на МОН.

§ 2. Разпоредбите на настоящите правила са задължителни за ДГ № 127 „Слънце”.

§ 3. Неразделна част от настоящите правила е образец на Приложение №7 от Наредба за минималните изисквания за мрежова и информационна сигурност

§4. Настоящите правила влизат в сила от датата на утвърждаването им.

§5. Вътрешните правила за мрежова и информационна сигурност са приети на заседание на ПС – Протокол № 1/15.09.2023 г. и са утвърдени със Заповед № 88/15.09.2023 г. на директора на ДГ № 127 ”Слънце”.