150. ОУ "Цар Симеон Първи"
адрес: гр. София, ж.к. "Дружба" - IV част, ул. "Делийска воденица" №11
телефон: 02 / 879 6663
e-mail: info-2207150@edu.mon.bg

УТВЪРДИЛ:/п/
Виолина Велкова-Иванова
Директор на 150.ОУ
“Цар Симеон Първи”

Политика
за мрежова и информационна сигурност
на 150.ОУ „Цар Симеон Първи и
вътрешни правила за МИС

В съответствие с изискванията на
Наредба за минималните изисквания за мрежова и информационна сигурност

(Документът интегрира политиката и правилата за нейното прилагане)

Политиката е приета на заседание на ПС, Протокол № 14/12.09.2025г. Утвърдена със заповед № РД 12-1115/12.09.2025г. на директора на училището

Актуализираната Политика е приета на заседание на ПС, Протокол № 3 / 29.01.2026г. и утвърдена със заповед № 521 / 29.01.2026г.

РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите политика и вътрешни правила се утвърждават на основание чл. 1, ал. 1, т. 1 от Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС № 186 от 26.07.2019 г.,) и имат за цел осигуряването на контрол и управление на работата на информационните системи в 150. ОУ „Цар Симеон Първи“ Настоящата политика за мрежова и информационна сигурност определя ред, отговорности, способи и средства при осъществяване контрол и управление на работата на информационните системи във 150.ОУ "Цар Симеон Първи", както и дейностите, които трябва да се предприемат, за отговор на всякакъв вид инциденти, свързани със сигурността на информационните активи и отрицателно въздействие върху поверителността, целостта и наличността на информацията. В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и 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. Потребителите на информационни системи в 150.ОУ “Цар Симеон Първи” са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3. Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Наредбата за минималните изисквания за мрежова сигурност.

РАЗДЕЛ II. КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

Чл.4. (1) Всяка информация, която стане достъпна за служителите при изпълнение на служебните им задължения, ако са свързани с училището и негова дейност, клиенти или партньори за сътрудничество, се счита за собствена и поверителна информация, 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.

(2). За да се установи подходяща защита на информацията, 150.ОУ "Цар Симеон Първи" извършва класификация на информацията. 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.

(3). Обща класификация на информацията, приложима в рамките на училището:

Ниво/ Етикетиране	Категория	Описание	Примери (неизчерпателни)
0 TLP–WHITE Не е нужно да се	Публична	Информация, която може да бъде обработвана и разпространявана в рамките на 150.ОУ "Цар Симеон Първи" или извън него без никакво отрицателно въздействие върху училището, някой от	(а) Финансови отчети, публикувани до обществени органи; (б) Информация, достъпна чрез публични ресурси или публично известна по друг начин, освен

обозначава		неговите партньори, и/или свързани лица. Поради общодостъпния си характер предполага анонимно ползване и не изисква средства за защита. Да се спазват стандартните правила за авторство.	ако не е станала обществено достояние вследствие на действия на служители в нарушение на правилата за защита на информацията.
1 TLP – GREEN	Вътрешна информация	Обменът в рамките на 150.ОУ е свободен. Информацията може да се споделя и с други публични организации, партньори и заинтересовани страни. Обмяната ѝ се извършва в рамките на споделени общности, но не по публични канали. Достъп се предоставя на конкретни лица, достъпващи с данни за идентификация	(а)Документи, разработени и/или изготвени от който и да е служител на училището; (б)Всички директории (информация за връзка и т.н.), установени и/или използвани за целите на училището; (в)Всякакви вътрешни работни бележки, изявления, становища, разработени за нуждите на училището или с цел ефективност на дейността.
2 TLP – AMBER	Поверителна информация	Всяка информация от такова значение за 150.ОУ "Цар Симеон Първи", който и да е от неговите партньори или свързани лица, неоторизираното разкриване, на която би могло да окаже неблагоприятно въздействие върху дейността, репутацията, цялостното състояние на училището и партньори, като последица от такова разкриване, която би причинила сериозни вреди/щети на някое от тези лица.	(а)Политики, процедури, вътрешни правила, управленски решения; (б)Информация, за която е указано на служителя, че е поверителна за училището; (в)Друга информация от финансово, кадрово, правно, маркетингово естество, планове и операции; (г)Данни за лична идентификация; (д)Информация, която подлежи на защита по силата на споразумение за поверителност, което се подписва от дадения служител; (е)Информация, която подлежи на защита по силата на споразумения за поверителност или споразумения за

			сътрудничество, които училището е сключило в хода на дейността си.

РАЗДЕЛ III. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 5. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

1. Разделяне на потребителски от администраторски функции.
2. Установяване на нива на достъп до информация.
3. Регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация.
4. Осъществяване на контрол
5. Техниката да се използва изключително и само за служебни цели.
6. Не се позволява инсталирането на какъвто и да е нов и реконфигурирането от потребителите на вече инсталиран софтуер и хардуер, както и самостоятелни опити за поправка или подобрения на горепосочените. При съмнение за възникнал проблем незабавно се уведомява ЗДУД.
7. Не се позволява използването на внесени отвън софтуер и хардуер.
8. Използването на внесени отвън информационни носители (оптични дискове, флаш памети и др.) става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, носителите не се използват.
9. Не се допускат външни лица до комуникационните шкафове и техниката за интернет-връзка, с изключение на техници от оторизирани фирми и то само придружени от ЗДУД.
10. Не се допуска достъпа на външни лица до компютърната техника в канцеларите в сградата на 150.ОУ “Цар Симеон Първи”.
11. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.
12. Паролите за достъп на всички служители, описани по видове приложения се съхраняват от ЗДУД. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 5. Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили.

Чл. 6. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез средствата на активна директория с конкретно потребителско име, осигурено от ЗДУД, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 7. Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заемната длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

Чл. 8. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн.

Чл. 9. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 10. Всички носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп.

Чл. 11. На служителите на 150.ОУ "Цар Симеон Първи", които използват електронни бази данни и техни производни се забранява:

- да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга);
- да ги използват извън рамките на служебните си задължения;
- да ги предоставят на външни лица без да е заявена услуга.

Чл. 12. За нарушение целостта на данните се считат следните действия:

- унищожаване на бази данни или части от тях;
- повреждане на бази данни или части от тях;
- вписване на невярна информация в бази данни или части от тях.

Чл. 13. При изнасяне на носители извън физическите граници на 150.ОУ "Цар Симеон Първи", те се поставят в подходяща опаковка и в запечатан плик.

Чл. 14. На служителите е строго забранено да използват служебни мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него.

Чл. 15. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл. 16. След като повече не са необходими, носителите се унищожават сигурно и безопасно за намаляване на риска от изтичане на чувствителна информация към неупълномощени лица. Физическото унищожаване на информационните носители става със счупване. Предварително се проверяват, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

Чл. 17. Събирането, подготовката и въвеждането на информацията на интернет страницата на училището се извършва от упълномощени служители. Длъжностните лица притежават потребителски имена и пароли за актуализиране на сайта.

РАЗДЕЛ IV. РАБОТНО МЯСТО

Чл. 18. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 19. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място.

Чл. 20. Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола.

Чл. 21. Забранява се на външни лица работата с персоналните компютри на 150.ОУ "Цар Симеон Първи", освен за:

- упълномощени фирмени специалисти в случаите на първоначална инсталация на

компютърна и периферна техника, програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствие на директор, заместник директор или ЗДУД;

- провеждане на обучения на външни педагогически специалисти по програми и проекти на МОН или РУО, но само след разрешението на директора на училището и задължително в присъствието на ЗДУД.

Чл. 22. След края на работния ден всеки служител задължително изключва компютъра, на който работи или го превежда в режим log off.

Чл. 23. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява ЗДУД, който му оказва съответна техническа помощ.

Чл. 24. Забраняват се опити за достъп до компютърна информация и бази данни, до които не са предоставени права, съобразно заеманата от служителя длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп.

Чл. 25. 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 ЗДУД.

Чл. 26. Забранява се използването на преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на 150.ОУ "Цар Симеон Първи".

Чл. 27. Служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

Чл. 28. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача. Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи - идентификация на потребител, пароли, отчитане на времето на достъп, забрани за копиране, проследяване на несанкциониран достъп.

Чл. 29. Достъпът до помещенията с комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

Чл. 30. С оглед да се намали рискът от нерегламентиран достъп, загуба или повреждане на информацията в работно и извън работно време, се прилага политика на „чисти бюра" и „чисти екрани". Информацията, оставена на открито върху бюрата, също така може да бъде повредена или разрушена по време на бедствия, като например пожар, наводнение и др.

Процесът предвижда следните мерки за контрол:

• Където е уместно, хартиените и електронните носители се съхраняват в подходящи затворени шкафове и/или метални каси, когато не се използват и по-специално в извън работно време.

• Чувствителната или важната информация е заключена отделно в огнеупорна каса, когато не е необходима, в частност, когато помещението е празно.

• Персоналните компютри и компютърни терминали и принтери не се оставят включени в системата, когато са оставени без наблюдение и са защитени посредством ключалки, пароли и други средства за контрол, когато не се използват.

• Местата с входяща и изходяща поща, които са оставени без наблюдение, са защитени.

• Копирните машини се заключват и са защитени от нерегламентирано използване в извън работно време.

• Чувствителната или класифицирана информация, когато се отпечатва, се сваля от принтерите незабавно.

Чл.31Работа от разстояние (съгл. чл.20 от НМИМИС)

(1)Работата извън помещенията на 150.ОУ "Цар Симеон Първи", следва да се извършва при спазване на допълнителни мерки за сигурност.

(2)Използването на лични устройства за служебни цели е допустимо единствено след изрично одобрение от директора. При такова одобрение е задължително прилагането на политики за управление на мобилни устройства (MDM), които гарантират, че устройството е актуализирано, защитено с антивирусен софтуер, криптиран диск и силни пароли, както и че може да бъде управлявано дистанционно при необходимост (например в случай на загуба или кражба).

(2)Забранява се свързване към публични или несигурни мрежи (например Wi-Fi точки на хотели, заведения и т.н.). Служителите са длъжни да използват собствени мобилни данни и да деактивират автоматичното свързване към безжични мрежи.

(3)При работа от разстояние служителите трябва да прилагат необходимите мерки за ограничаване на достъпа до устройствата (служебни или лични), като не ги оставят без надзор на публични пространства (кола, маса в заведение и т.н.), заключват екрана при отсъствие и не разрешават достъп на трети лица (приятели, познати, роднини) до тях.

(4)Служителите следва да имат предвид, че дистанционният достъп се наблюдава и контролира, а всички действия, извършени през служебните системи, се регистрират с цел гарантиране на сигурността, отчетността и съответствието с вътрешните правила и действащото законодателство. Нарушения на тези изисквания подлежат на санкции и търсене на дисциплинарна отговорност.

Чл.32. Мобилни устройства

(1)Мобилните устройства – включително телефони, лаптопи, таблети и преносими носители на информация (USB памети, външни твърди дискове и др.), съхраняващи и обработващи служебна информация, са рисков актив за сигурността. Поради това тяхното използване следва да се извършва при спазване на строги правила за МИС.

(2)Всички устройства са защитени със силна парола, PIN код (от поне 4 знака) или биометрични данни като пръстов отпечатък или лицево разпознаване.

(3)Цялата чувствителна или служебна информация, съхранявана на мобилни устройства или външни носители, е криптирана. Не се допуска съхранение на служебни данни в не криптирани папки или в лични облачни услуги.

(4)При загуба, кражба или съмнение за компрометиране на устройство, служителят е длъжен незабавно да уведоми директора на училището.

(5)Използването на USB памети, външни дискове и други преносими носители е ограничено и се допуска само след предварително одобрение. Чувствителната информация, съхранявана върху такива носители, подлежи на задължително криптиране. Лични външни устройства не се свързват със служебни компютри или мрежи, тъй като това може да доведе до компрометиране на сигурността.

(6)Редовното актуализиране на операционните системи, антивирусния софтуер и приложенията

на всички мобилни устройства е задължително. Забранено е инсталирането на непозволени приложения, които могат да представляват риск за информационната сигурност.

(7)При пренасяне на лаптопи и външни носители извън офиса те трябва да се съхраняват в защитени чанти, куфари или багажника на автомобил, за да се намали рискът от кражба или повреда.

(8)Преди изваждане от експлоатация на устройство се извършва неговото пълно прочистване със сертифицирани софтуерни инструменти. По преценка на оторизиран представител на фирмата за поддръжка на техниката на училището устройството може да бъде физически унищожено, чрез раздробяване, пробиване и тн., което се документира с протокол.

Чл.33. Чисто бюро и чист екран

(1)Политиката за чисто бюро и чист екран има за цел да гарантира защитата на информацията и предотвратяване на неоторизиран достъп до служебни данни и активи. Всички служители носят отговорност да спазват добри практики, които намаляват риска от изтичане на чувствителна информация.

(2)При отсъствие от работното място, дори и за кратък период от време, служителите са длъжни да заключват компютрите си. Освен това всички устройства следва да бъдат настроени за автоматично заключване след определен период на неактивност, за да се предотврати достъп от неоторизирани лица.

(3)Бюрата трябва да бъдат освободени от всякакви видове документирана информация, с която служителят не работи текущо и може да бъде разкрита пред неоторизирани лица. Всички документи и преносими носители, които съдържат чувствителна или поверителна информация, трябва да се съхраняват в заключени шкафове, когато не се използват. Не се допуска оставянето им на бюрата без надзор. Забранява се записването на пароли за достъп до системи на хартиен носител.

(4)Служителите следва да проявяват особено внимание към видимостта на екрана си при работа, особено в помещения с повече хора или на обществени места. Екраните трябва да бъдат разположени така, че да се намали рискът от визуален достъп от трети лица. Мониторите трябва да бъдат свободни от стикери с пароли и други типове чувствителна информация. Върху началните екрани не трябва да бъда се запазват файлове с пароли и друга чувствителна информация, които могат лесно да бъдат достъпени.

Чл.34. Пароли и автентикация

(1)Паролите са основен елемент за защита на информационните системи и достъп до служебни ресурси. Тяхното правилно управление е критично за предотвратяване на неоторизиран достъп, загуба на данни и компрометиране на сигурността. Всички служители са длъжни да спазват следните правила и добри практики за създаване, използване и съхранение на пароли.

(2)Минималните изисквания за сигурна парола (на обикновените потребители) включват:

• дължина не по-малка от 8 символа;

• комбинация от главни и малки букви, цифри и специални символи;

• уникалност на паролата за всяка система или приложение.

(3)Паролите трябва да бъдат редовно сменяни, като се препоръчва смяна поне веднъж на всеки 6 месеца или незабавно при съмнение за компрометиране. При получаване на първоначален достъп до система, паролата за достъп трябва задължително да се смени. Служителите трябва да избягват използването на една и съща парола за служебни и лични акаунти, както и пароли, които

могат лесно да бъдат отгатнати (например имена на близки, дати на раждане, телефонни номера или често срещани думи).

(4)Паролите не се записват на хартия, не се съхраняват в некриптирани файлове и не се споделят с колеги или външни лица при никакви обстоятелства. В случай на необходимост от предоставяне на достъп се използват официалните механизми за управление на права, а не споделяне на идентификационни данни. Потребителите носят пълна отговорност за съхранението на използваните от тях пароли.

Чл.35 Използване на изкуствен интелект

(1)150.ОУ "Цар Симеон Първи" насърчава отговорното и внимателно използване на платформи, базирани на изкуствен интелект (ИИ) като помощен инструмент в ежедневната работа на служителите.

(2)Изкуствен интелект може да се използва за облекчаване на оперативните задачи на служителите, езикови услуги и подобряване на качеството на служебна кореспонденция при условие, че служителят не изнася чувствителна информация за училището и служителите.

(3)При използване на ИИ е забранено въвеждането на информация с ниво 2 и лични данни на граждани и служители. Забранено е използването на ИИ за нарушаване на авторско право или създаване на съдържание, неотговарящо на етичния кодекс на 150.ОУ "Цар Симеон Първи".

(4)Служителите следва да проявяват критично мислене и бдителност при използване на информацията, предоставена от ИИ. Препоръчително е информацията да бъде проверявана в друг независим източник.

РАЗДЕЛ IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 36. Компютрите, свързани в мрежата на 150.ОУ “Цар Симеон Първи”, използват интернет само от доставчик, с когото училището има сключен договор за доставка на интернет.

Чл. 37. Фирмата, доставчик на интернет услугата, изгражда вътрешна мрежа с необходимите мрежови комутатори, VLAN, рутери, защитни стени, VPN; избира техническите устройства, извършва необходимите настройки за достъп до интернет, разделя логически локалната мрежа на четири отделни мрежи – локална мрежа за администрация, локална мрежа за учители, локална мрежа за ученици и локална мрежа за гости и създава потребителски имена и пароли за работа с компютърната мрежа.

Чл. 38. Ползването на компютърната мрежа и електронните платформи /Школо, Уча се, Електронни учебници и др./ от служителите става чрез получените потребителско име и парола.

Чл. 39. Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.

Чл. 40. Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронните платформи при използване на предоставените им потребителски имена и

пароли.

Чл. 41. Забранява се свързването на компютри едновременно в мрежата на 150.ОУ "Цар Симеон Първи" и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на училището и/или е в противоречие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл. 42. Използването на комуникатори (skype, facebook, messenger, viber, zoom и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на 150.ОУ "Цар Симеон Първи" и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на училището, да е ограничено и единствено и само за служебна цел.

Чл. 43. Забранява се съхраняването на компютрите на 150.ОУ "Цар Симеон Първи" на лични файлове с текст, изображения, видео и аудио.

Чл. 44. Забранява се отварянето без контрол от страна на служителите с достъп до електронната поща на училището на:

- получени по електронна поща или на преносими носители изпълними файлове, файлове с мобилен код и файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg и архивни файлове;получени по електронна поща съобщения, които съдържат неразбираеми знаци.

Чл. 45. Не се толерира влизането в Интернет - сайтове с неизвестно съдържание.

РАЗДЕЛ V. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 46. С цел антивирусна защита се прилагат следните мерки:

- Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява.
- Ръководителят на направление „ИКТ" извършва следните дейности:

- активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;
- настройва антивирусния софтуер за периодични сканирания през определен период;
- активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система;
- проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер.

- При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира ЗДУД.

РАЗДЕЛ VI. НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 47. Следните мерки се прилагат с цел антивирусна защита:

1. Всички устройства за съхранение на данни да са свързани към устройство за непрекъсваемост на ел. снабдяването.

2. При липса на ел. захранване за повече от 10 мин., ЗДУД започва процедура по поетапно спиране на устройствата за съхранение на данни.

3. При срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация.

РАЗДЕЛ VII СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 48. Всеки служител, който работи с класифицирана информация, осигурява автоматично създаване на архивни копия всекидневно.

Чл. 49. Информацията, включително тази, съдържаща лични данни, се резервира по следните начини:

1. Автоматизирано и планово се извършва архивиране на цялата работна информация на запаметяващите устройства и дисковите масиви.

2. Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг компютър и да се продължи работният процес без чувствителна загуба на данни.

РАЗДЕЛ VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в 150.ОУ “Цар Симеон Първи” са длъжни да познават и спазват разпоредбите на тази политика.

§ 2. Контролът по спазване на правилата за работа, основани на Политиката за мрежова и информационна сигурност се осъществява от ръководството на 150.ОУ „Цар Симеон Първи“

§ 3. Настоящата политика се разглеждат и оценява периодично с оглед ефективността й, като 150.ОУ “Цар Симеон Първи” може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Политиката за МИС и правилата за работа, основани на нея са разработени съгласно Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС № 186 от 26.07.2019г.).