

**38 ОУ “Васил Априлов”, гр. София**

# **ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ**

<b>Версия 1.1</b>	<b>Утвърдил: .....</b>
<b>Дата: 01.04.2022</b>	<b>Мариета Димитрова Директор</b>

# СЪДЪРЖАНИЕ

I. ОБЩИ ПОЛОЖЕНИЯ .....	3
II. ОБЩИ МЕРКИ ЗА СИГУРНОСТ .....	3
III. МЕРКИ ЗА СИГУРНОСТ ПРИ РАБОТА НА СЛУЖИТЕЛИТЕ С ИНФОРМАЦИОННИТЕ РЕСУРСИ.....	6
IV. АНАЛИЗ, ОЦЕНКА НА РИСКА И УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ АКТИВИ .....	7
V. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ .....	7

# I. ОБЩИ ПОЛОЖЕНИЯ

**Чл.1.** Настоящата политика има за цел осигуряването на мрежова и информационна сигурност в 38 ОУ “Васил Априлов”.

**Чл.2.** Мрежовата и информационна сигурност се осигурява чрез следните мерки:

1. Организационни мерки;
2. Технологични мерки;
3. Технически мерки;

**Чл.3.** Мерките, които 38 ОУ “Васил Априлов” прилага във връзка с осигуряването на мрежова и информационна сигурност са насочени към запазване на достъпността, наличността и конфиденциалността на информацията по време на целия ѝ жизнен цикъл, включващ създаването, обработването, съхранението, пренасянето и унищожението ѝ в и чрез информационните и комуникационните системи на училището и ползваните от него външни системи.

**Чл.4.** Във 38 ОУ “Васил Априлов” за мрежовата и информационната сигурност е отговорен главният информатик, като:

1. С оглед на спазването на всички изисквания, служителят е на пряко подчинение на директора на училището и пряко го информира за състоянието и проблемите в мрежовата и информационната сигурност;
2. Препоръчителни функции на служителят, отговарящ за мрежовата и информационната сигурност, са описани в приложение № 6 от Наредбата за минималните изисквания за мрежова и информационна сигурност (Наредбата).

# II. ОБЩИ МЕРКИ ЗА СИГУРНОСТ

**Чл.5.** За осигуряването на мрежова и информационна сигурност, главният информатик е необходимо да предприема следните минимални мерки по отношение на използваните информационни ресурси:

- (1) Всички рутери, Wi-Fi устройства използвани за осигуряване на мрежовата свързаност и интернет, и устройства за осигуряване на видеонаблюдение на територията на училището е необходимо да бъдат поставени в помещения с ограничен достъп, достъп до които да имат само оторизирани лица.
- (2) За защита до софтуера за управление на рутерите и достъп до системите за видеонаблюдение е необходимо да се прилагат пароли, които да отговарят на следните минимални изисквания за сигурност: използване на главни и малки букви,

използване на специални знаци, минимална дължина на паролата 8 символа и смяна на паролите поне веднъж годишно и във всеки случай, в който е била получена информация за компрометиране на достъпа.

- (3) При осигуряването на безжичен Wi-Fi интернет, задължително се осигурява разделение на мрежите използвани от преподавателския и изпълнителския персонал и мрежата използвана от учениците, ако такава се осигурява от училището.
- (4) Wi-Fi мрежата, използвана за служебни цели, задължително се защитава с парола, която трябва да бъде сменяна поне веднъж годишно в началото на учебната година и във всеки случай, в който постъпи информация че е компрометирана.
- (5) Допустимо е безжичната мрежа за учениците да е Guest и да не е защитена с парола, при условие, че е спазено задължителното условие мрежата да е отделена от останалите мрежи в училище.
- (6) Разделянето на мрежите се допуска да бъде както хардуерно, така и софтуерно на ниво рутер или друго устройство, ползвано за настройка на мрежите и входящия интернет.
- (7) Задължително и необходимо е да се прилагат политики (чрез софтуерни настройки на мрежовите устройства) по отношение на достъпа до неподходящо съдържание, както и до съдържание водещо до риск от заразяване на мрежите с вируси и погубване на информация.
- (8) Системата за видеонаблюдение на територията на училището, е допустимо да е свързана само към мрежата използвана за служебни цели, или отделна мрежа, отделена от основната чрез хардуерен или софтуерен способ.
- (9) Информацията за всички настройки и пароли за достъп до мрежовото оборудване е допустимо да се съхранява в електронен вид чрез специализиран софтуер за целта, който да гарантира сигурността на данните. Препоръчително е достъп до данните да имат още минимум едно лице, освен главния информатик, като лицето се определя чрез заповед.
- (10) При използването на външен доставчик за поддръжка и осигуряване на мрежовата свързаност и видеонаблюдение, отговорността за прилагането на общите мерки по чл.5, както и достъпът и съхранението на данните за настройки и пароли са отговорност на доставчика, като за целта това е необходимо да бъде разписано в договора на съответния доставчик.

**Чл.6.** За осигуряването на сигурността на информацията, създавана, обработвана, архивирана и пренасяна в специализирани за целта софтуерни продукти главният информатик, е необходимо да предприема следните минимални мерки по отношение на използваните информационни ресурси:

- (1) На всички сървъри, служебни компютри и мобилни устройства се използват само лицензирани операционни системи и софтуерни продукти.
- (2) При използването на Windows операционна система, е необходимо с цел осигуряването на защита на устройствата да е активиран минимум Windows Defender, да са включени опциите за автоматичен update.

- (3) Всички компютри и мобилни устройства, които са предназначени за общо ползване в т.ч. разположените в общите помещения и учителската стая се използват само “Guest mode” с настройка на изтичането на сесията след определено време в което потребителя е неактивен.
- (4) В съответствие със спазването на регламента за защита на личните данни GDPR, Закона за защита на личните данни и вътрешните за училището правила, политики и инструкции за защита на личните данни е задължително да се прилагат мерки по защита на ключовите бази данни на училището, като се осигурява архивиране на данните и защита от неоторизиран достъп.
- (5) За защита на данните в използвания специализиран софтуер в училището е необходимо да се прилагат пароли, които да отговарят на следните минимални изисквания за сигурност: използване на главни и малки букви, използване на специални знаци, минимална дължина на паролата 8 символа и смяна на паролите поне веднъж годишно и във всеки случай, в който е била получена информация за компрометиране на достъпа.
- (6) Достъпът за администриране на специализирания софтуер, използван в училището и данните в него в т.ч. Admin Pro, Admin RD, използваните външни системи за обмен на информация, в т.ч. НЕИСПУО и администрирането на платформите за обучение shkolo.bg, Microsoft Teams, Google Class Room и др. се осъществява само от оторизирани за това лица.
- (7) Лицата по чл. 6, т. 6. се определят от директора на училището чрез заповед или чрез разписани в длъжностна характеристика задължения на служителите отговорни за администриране на системите.
- (8) За да се предотврати загуба на данни е необходимо да се осигурят мерки за архивиране на информация, когато такива не са предоставени от производителя или внедрителя на софтуера и това не е регламентирано в договор.
- (9) Мерките за архивиране на данните, трябва да са такива, че да осигуряват архив на данните на различно физическо устройство, от това на което се използва продуктивната база данни.

**Чл.7.** За намаляване на загубите от инциденти, чрез намаляваме на времето за реагиране и разрешаването им, както и за намаляване на вероятността от инциденти, породени от човешки грешки, главният информатик поддържа следната документация:

- (1) Регистър на информационните активи – списък на наличния хардуер и софтуер;
- (2) Физическа схема на свързаност;
- (3) Логическа схема на информационните потоци;
- (4) Документация на структурната кабелна система;
- (5) Техническа и потребителска документация на мрежата и информационната система;

**Чл.8.** Документацията по чл. 11 следва да е еднозначно идентифицирана като заглавие, версия, дата, автор и номер. Документацията може да се води на електронен или хартиен носител, като се актуализира минимум веднъж годишно и се утвърждава от директора на

училището, а достъп до нея имат само главния информатик, директорът на училището и оторизираните за това лица, назначени чрез заповед или договор.

### **III. МЕРКИ ЗА СИГУРНОСТ ПРИ РАБОТА НА СЛУЖИТЕЛИТЕ С ИНФОРМАЦИОННИТЕ РЕСУРСИ**

**Чл.9.** 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.10.** На служителите на училището е строго забранено да използват мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него. Потребителите на мобилни компютърни средства и мобилни телефони отговарят за защитата им от кражба и не ги оставят без наблюдение.

**Чл.11.** При извършване на работа от разстояние служителите на училището спазват всички изисквания за осигуряване защитата на данните, в т.ч. лични данни на трети лица и/или по класификацията на информацията.

**Чл.12.** Забранява се използването на служебни и мобилни устройства при осъществяване на дистанционен достъп от публични незащитени мрежи (мрежи в молове, заведение и др.) , освен в случаите когато достъпът се осъществява през защитена VPN връзка, осигурена от училището.

**Чл.13.** При използването на специализиран софтуер и използването на предоставени външни системи за работа в т.ч. shkolo.bg, Microsoft Teams, Google Class Room и др. е необходимо да се прилагат пароли, които да отговарят на следните минимални изисквания за сигурност: използване на главни и малки букви, използване на специални знаци, минимална дължина на паролата 8 символа и смяна на паролите поне веднъж годишно и във всеки случай в който е била получена информация за компрометиране на достъпа.

**Чл.14.** Паролите за достъп до служебните компютри и програмни продукти, се съхраняват от самите служители, като е забранено да бъдат предоставяни на други лица.

**Чл.15.** Паролите за достъп до общи служебни ресурси в т.ч. достъп за безжичната мрежа и интернет, е забранено да се предоставят на външни лица и учениците, освен в случаите когато това е разрешено със заповед на директора или чрез договор.

**Чл.16.** При установен случай на изтичане на информация и пароли, служителят е длъжен незабавно да уведоми главния информатик и директора, за да бъдат предприети незабавни действия, по реда на чл. 8 и чл. 9 от настоящия документ.

**Чл.17.** Не се позволява инсталирането на какъвто и да е нов и реконфигурирането от потребителите на вече инсталиран софтуер и хардуер, освен с разрешение на главния информатик или от самия него.

**Чл.18.** Използването на внесени отвън информационни носители(оптични дискове, дискети, флаш памет и др.) става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, носителите не се използват; При работа с USB флаш памет, дискове или дискети, наличната информация, която е лична е необходимо да се копира и пренесена в рамките на училищната мрежа, използван софтуер или cloud услугите използвани от училището след което данните е необходимо да бъдат унищожени. Допуска се съхраняването на лични данни на преносим носител, само в случаите когато същия се съхранява в заключена каса при директора или оторизирани от него служебни лица.

**Чл.19.** Инсталирането на софтуерни програми, несъотнесими към пряката служебна работа е забранено;

**Чл.20.** Забранено е тегленето на файлове с неизвестно съдържание от Интернет;

**Чл.21.** Служителите не трябва да отварят съобщения, получени от неизвестен получател или неизвестна Интернет страница. Такива съобщения се изтриват незабавно;

**Чл.22.** Прикачените файлове към съобщенията, получени в служебните пощи, не се отварят при съмнение за вируси;

**Чл.23.** Потребителите на информационни системи в 38 ОУ “Васил Априлов” са задължени с отговорни действия да гарантират ефективното и безопасно използване на системите.

## **IV. АНАЛИЗ, ОЦЕНКА НА РИСКА И УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ АКТИВИ**

**Чл.24.** Управлението на риска за сигурността на информационните и комуникационните системи се извършва минимум веднъж годишно, съгласно вътрешната процедура за анализ и оценка на риска.

**Чл.25.** Управлението на информационните активи се извършва съгласно счетоводната политика и правила приети в училището за управление на активите.

## **V. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ**

**Чл.26.** Служителите в 38 ОУ “Васил Априлов” са длъжни да познават и спазват разпоредбите на настоящата Политика.

**Чл.27.** Настоящата Политика за мрежова и информационна сигурност се разглежда и оценява периодично с оглед ефективността ѝ, като 38 ОУ “Васил Априлов” може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

**Чл.28.** Настоящата политика е разработена в съответствие с регламента на ЕС за защита на личните данни GDPR, Закона за защита на личните данни и вътрешните за училището правила, политики и инструкции за защита на личните данни, както и Наредбата за минималните изисквания за мрежова и информационна сигурност и е утвърдена със заповед на директора на училището 473/05.02.2021г.

## **VI. ВЕРСИИ НА ДОКУМЕНТА**

**В настоящата версия 1.1 добавени следните промени:**

В чл. 18 е добавен следния текст: *„При работа с USB флаш памети, дискове или дискети, наличната информация, която е лична е необходимо да се копира и пренесена в рамките на училищната мрежа, използван софтуер или cloud услугите използвани от училището след което данните е необходимо да бъдат унищожени. Допуска се съхраняването на лични данни на преносим носител, само в случаите когато същия се съхранява в заключена каса при директора или оторизирани от него служебни лица.“*