106 ОСНОВНО УЧИЛИЩЕ "ГРИГОРИЙ ЦАМБЛАК"
гр. София, район "Подуяне", ул. "Григорий Цамблак" №18, п.к.1517
тел. 028472181; 029452879; e-mail: ou106g.camblak@abv.bg ; www.ou106.info

Приложение 1

Утвърждавам.....

Ирена Милева-Цукева
Директор на 106 ОУ „Григорий Цамблак"

ПРАВИЛА

ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

В 106 ОУ"Григорий Цамблак

РАЗДЕЛ I ОБЩИ ПОЛОЖЕНИЯ

Чл. 1 (1) Настоящите 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 19.07.2019г.,) и имат за цел осигуряването на контрол и управление на работата на информационните системи в 106 ОУ „Григорий Цамблак". 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.

(2) Правилата са разработени в съответствие със Закона за киберсигурност, Наредба за минималните изисквания за мрежова и информационна сигурност, наричана по- долу НМИМИС, както и със Закона за електронното управление, Закона за електронната идентификация, Закона за електронните съобщения, Наредбата за електронните административни услуги и други.

(3) Правилата са част от политиката за мрежова и информационна сигурност на 106 ОУ и целят защитата на информационните мрежи и системи срещу неправомерен или случаен достъп, използване, правене достояние на трети лица, промяна или унищожаване, доколкото такива събития или действия могат да нарушат достъпността, автентичността, целостта, интегритета и конфиденциалността на съхраняваните или предаваните данни, а също така на предоставяните електронни услуги, свързани с тези мрежи и системи.

(4) 106 ОУ предприема необходимите технически и административни мерки за защита на информационните мрежи и системи, съобразно спецификата на административните процеси.

Решенията за мрежова и информационна сигурност се изграждат за осигуряване на всяко от следните нива:

1. мрежи;
2. системи;
3. приложения;
4. информация.

(5) За всяко от нивата по ал.2 се осигурява съответният контрол с цел да се обезпечи адекватно ниво на сигурност, като се прилагат разписаните принципи в НМИМИС.

Чл. 2 Потребителите на информационни системи в 106 ОУ „Григорий Цамблак“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 (приета с ПМС № 186 от 19.07.2019г.).

РАЗДЕЛ II
ОРГАНИЗАЦИЯ НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ

Чл.4.(1) Директорът отговаря за мрежовата и информационна сигурност в 106 ОУ, като взема необходимите документирани решения, чрез утвърждаването на политики, правила, процедури и други, както и чрез осигуряване на необходимата инфраструктура за гарантиране на мрежовата и информационна сигурност на използваните информационни мрежи и системи.

(2) Отговорностите на служителите за гарантиране на мрежовата и информационна сигурност на използваните информационни мрежи и системи се определят в длъжностните им характеристики или работни планове, както и на друго документирано основание.

(3) Директорът определя лице, отговарящо за мрежовата и информационна сигурност в 106 ОУ „Григорий Цамблак", на пряко негово подчинение. Функциите на лицето, отговарящо за мрежовата и информационната сигурност, са разписаните в НМИМИС.

(4) Директорът възлага на Заместник директор по УД контрола по изпълнението на взетите документирани решения за гарантиране на мрежовата и информационна сигурност на използваните информационни мрежи и системи.

(5) Директорът организира комплексни проверки за оценяване степента на постигнатата мрежова и информационна сигурност в използваните в 106 ОУ информационни мрежи и системи.

РАЗДЕЛ III
ОЦЕНКА И УПРАВЛЕНИЕ НА РИСКА

Чл.5.(1) С настоящите Правила се определят основните действия по оценка и управление на риска за мрежовата и информационна сигурност в 106 ОУ, както и идентифициране на потенциалните рискови фактори във връзка с нея.

(2) Рискът за сигурността се определя като фактическо състояние, създаващо заплахи за уязвяване на един или няколко информационни актива, което предизвика тяхното повреждане или унищожаване.

(3) Оценката на риска се определя чрез изчисление на вероятността за уязвяване въз основа на ефективността на съществуващите или планираните мерки за сигурност.

(4) Действията по управление на риска 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 периодично повтарящи се действия:

1. оценка (преоценка) на риска;

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

Чл.6. При идентифициране на риска се предприема едно от следните действия:

1. ликвидиране на риска, чрез отстраняване на причиняващите го обстоятелства;

2. намаляване на риска, чрез използване на допълнителни защитни средства;

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

Чл.7.(1) Процесът на управление на риска включва следните етапи:

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

2. избор на методология за оценка на риска;

3. идентификация на информационите 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;. оценка на резултативния риск.

(2) Процесът на управление на риска следва периодичност, като последният етап е нов цикъл на оценка, който се провежда:

1. ако резултативния риск е определен като неудовлетворителен;

2. с определената ежегодна периодичност.

Чл.8.(1) Заплахите за мрежовата и информационната сигурност се класифицират по следните критерии:

1. по елементите на мрежовата и информационната сигурност – достъпност, автентичност, целостта, интегритет и конфиденциалност, към които са насочени;

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

3. по начина на осъществяване – случайни или преднамерени действия, от природен или технологичен характер и други;

4. по разположението на източника – вътре или извън информационната система.

(2) Потенциалните рискови фактори за мрежовата и информационната сигурност, които могат да застрашат достъпността, автентичността, целостта, интегритета и конфиденциалността, са както следва:

1. подслушване и електромагнитно излъчване;

2. нежелан код и маскиране на потребителската идентичност;

3. погрешно насочване или пренасочване на съобщенията, както и липса на потвърждаване;

4. софтуерни грешки;

5. нерегламентиран достъп до информационните активи, повреждане, кражба и злоупотреба с тях;

6. грешки при поддръжката;

7. грешки при предаването на информация;

8. употреба на нерегламентирани програми и информация;

9. потребителски грешки;

10. претоварване на комуникационния трафик;

11. технически аварии и аварии в комуникационното оборудване, аварии в електрозахранването и климатичните инсталации, природни бедствия и външни въздействия с огън, вода, химикали и други.

Чл.9.(1) Идентифицирането, оценката и действията по управление на риска за мрежовата и информационна сигурност се осъществяват от лицето, отговорящо за мрежовата и информационна сигурност.

(2) Чрез оценката на риска за мрежовата и информационна сигурност се цели идентифицирането на неприемливите опасности, за които се налага да бъдат предприети съответните действия, както и върху опасностите, които са на приемливо ниво, за да се упражни контрол същите да останат в тези граници.

(3) Съобразно резултатите от извършената оценка, лицето, отговарящо за мрежовата и информационна сигурност избира реакция по отношение на всеки от рисковете като определя контролните цели и действия, за да даде увереност, че неприемливите рискове за мрежовата и информационна сигурност са ограничени до приемливи нива.

РАЗДЕЛ IV
ИНВЕНТАРИЗАЦИЯ НА ИНФОРМАЦИОННИТЕ АКТИВИ

Чл.10.(1) Предприемат се необходимите действия за създаване и поддържане на инвентарни списъци на наличните информационни активи в 106 ОУ.

(2) За инвентарен списък се считат вписаните данни в регистъра на информационните ресурси, воден от фирмата, обслужваща компютърната техника и мрежи на училището.

(3) Информационни активи са:

1. хардуерните устройства;

2. софтуерните продукти;

3. информационните системи;

4. комуникационната инфраструктура.

Чл.10. В картите на наличните информационни ресурси в 106 ОУ се определят еднозначно:

1. конкретен служител отговаря за конкретни информационни ресурси – работни станции, устройства, софтуерни продукти, информационни системи, бази данни и други;

2. конкретен софтуерен продукт, информационна система и база данни се използват на конкретни работни станции и устройства.

Чл.11. Инвентарните списъци за наличните информационни ресурси в 106 ОУ включват минималния набор от данни разписан в НМИМИС.

Чл.12. Според мястото и начина на поддръжка информационните системи в 106 ОУ са:

1. разположени на локални работни станции;

2. разположени на сървъри в локалната мрежа;

3. разположени на външни сървъри;

4. външни системи, в които се поддържа информация от служителите на 106 ОУ;

5. външни системи, ползвани от служителите със специални права.

РАЗДЕЛ V

КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл.13 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. Техниката да се използва изключително и само за служебни цели.
5. 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 Зам. директор по УД
6. Не се позволява използването на внесени отвън софтуер и хардуер.
7. Използването на внесени отвън информационни носители (оптични дискове, дискети, 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.
8. 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 Зам. директор по УД. Не се допуска достъпа на външни лица до компютърната техника в канцеларите в сградата на 106 ОУ „Григорий Цамблак“.
9. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.
10. Паролите за достъп на всички служители, описани по видове приложения, се съхраняват от Зам. директор по УД. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 14 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. 15 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 Зам. директор по УД, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 16 Предоставянето на достъп става, 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. 17 Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн;

Чл. 18 Всички пароли за достъп на системно ниво се променят периодично;.

Чл. 19 Всички носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп.

Чл. 20 На служителите на 106 ОУ „Григорий Цамблак“, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици) се забранява:

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

Чл. 21 За нарушение целостта на данните се считат следните действия:

1. унищожаване на бази данни или части от тях;
2. повреждане на бази данни или части от тях;
3. вписване на невярна информация в бази данни или части от тях.

Чл. 22 Изнасяне на носители извън физическите граници на 106 ОУ „Григорий Цамблак“ е разрешено за служебни цели.

Чл. 23 На служителите 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. 24 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. 25 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 проверят, за да е сигурно, че необходимата информация е копирана и съхранена.

РАЗДЕЛ VI

РАБОТНО МЯСТО

Чл.26 Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл.27 Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място.

Чл.28 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.29 Забранява се на външни лица работата с персоналните компютри на 106 ОУ, 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 преподавател по „ИКТ".

Чл.30 След края на работния ден всеки служител задължително изключва компютъра, на който работи.

Чл.31 При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Зам. директор по УД.

Чл.32 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.33 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 със ЗДАСД.

Чл.34 Забранява се използването на преносими непроверени за вируси магнитни, оптични и други носители върху компютри, свързани в компютърната мрежа на 106 ОУ.

Чл.35 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.36 Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача.

Чл.37 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.38 Достъпът до помещенията с комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

РАЗДЕЛ VII
ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.39 ЗДУД, съвместно с обслужващата компютърните мрежи фирма, извършват необходимите настройки за достъп до интернет, разделя логически локалната мрежа на три отделни мрежи – локална мрежа за администрация, локална мрежа за учители и локална мрежа за ученици. Създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща на 106 ОУ.

Чл.40 Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола.

Чл.41 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.42 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 електронна поща при използване на предоставените им потребителски имена и пароли.

Чл.43 Компютрите, свързани в мрежата на 106 ОУ използват интернет само от доставчици, с които 106 ОУ има сключен договор за доставка на интернет.

Чл.44 Забранява се свързването на компютри едновременно в мрежата на 106 ОУ и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на 106 ОУ и/или е в противоречие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл.45 Забранява се инсталирането и използването на комуникатори (като skype, facebook, messenger, viber и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на 106 ОУ 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 106 ОУ.

Чл.46 Забранява се съхраняването на компютрите на 106 ОУ на лични файлове с текст, изображения, видео и аудио.

Чл.47 Забранява се отварянето без контрол от страна на системния администратор:

1. 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;
2. получени по електронна поща съобщения, които съдържат неразбираеми знаци;

РАЗДЕЛ VIII
ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.48 С цел антивирусна защита се прилагат следните мерки

(1) Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.

(2) ЗДУД, съвместно с обслужващата компютърната техника фирма, извършва следните дейности:

2.1. активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;

2.2. настройва антивирусния софтуер за периодични сканирания през определен период, но поне веднъж седмично.

2.3. активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система;

2.4. проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер;

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

РАЗДЕЛ IX
НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл.49 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, се започва процедура по поетапно спиране на устройствата за съхранение на данни.

4. 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 X
СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл.50 Всеки служител, който работи с класифицирана информация, осигурява автоматично създаване на архивни копия всекидневно.

Чл.51 Информацията, включително тази, съдържаща лични данни, се резервира по следния начин:

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;

(4) Споделените документи се резервират ежедневно.

(5) Резервните копия се съхраняват на носител, различен от този, на който са разположени данните или електронните документи.

(6) Съхраняват се най-малко последните три резервни копия.

(7) Резервните копия се изпитват за консистентност и интегритет чрез пробно възстановяване на данни най-малко веднъж месечно.

РАЗДЕЛ XI
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в 106 ОУ са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от ръководството на 106 ОУ

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността й, като 106 ОУ може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС № 186 от 19.07.2019г.) и са утвърдени със Заповед № РД 570 на Директора на 106 ОУ "Григорий Цамблак".