



УТВЪРДИЛ!
Мустафа Бандьо:
Директор на Об.У „Иван Вазов“

ПОЛИТИКА
ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ
НА ОБЕДИНЕНО УЧИЛИЩЕ „ИВАН ВАЗОВ“ СЕЛО ПАШОВИ

РАЗДЕЛ I ОБЩИ ПОЛОЖЕНИЯ

Чл.1. Настоящата политика има за цел осигуряването на мрежова и информационна сигурност в Обединено училище „Иван Вазов“ село Пашови.

Чл.2. Мрежовата и информационна сигурност се осигурява чрез мерки, пропорционални на рисковете за постигането на основните цели:

1. организационни мерки;
2. технологични мерки;
3. технически мерки;

Чл.3. Мерки, които Обединено училище „Иван Вазов“ село Пашови прилага във връзка с осигуряването на мрежова и информационна сигурност са насочени към запазване на достъпността, интегритета (цялост и наличност) 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.

Чл.4. (1) В Обединено училище „Иван Вазов“ село Пашови за мрежовата и информационната сигурност е отговорен учителя по ИТ в Обединено училище „Иван Вазов“ село Пашови, 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).

Чл.5. Настоящата политика се преразглежда редовно, но не по-рядко от веднъж годишно, и при необходимост се актуализира.

Чл.6. 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.7. 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.8. 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.9. Криптографските механизми, които се използват от Училището са съобразени с уязвимостта на информацията към заплахи за нейните конфиденциалност и интегритет и с нормативните и регулаторните изисквания към нейното създаване, съхраняване и пренасяне.

Чл.10. (1) Всеки служител на Обединено училище „Иван Вазов“ село Пашови 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.

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

Чл.11. При разработването на нови информационни и комуникационни системи от Училището се спазват всички изисквания на Наредбата така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда.

Чл.12. (1) С цел да се намалят загубите от инциденти чрез намаляване на времето за реагиране и разрешаването им, както и за намаляване на вероятността от възникване на инциденти, породени от човешки грешки, училището поддържа следната документация:

1. опис на информационните активи – поддържа се актуален в регистъра на информационните ресурси на ДАЕУ от касиер-домакина на училището;
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 комуникационни 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

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, факс, използване на сменяеми носители на информация в електронен вид, използване на преносими записващи устройства и т. н.

(2) Документацията по ал. 1 е:

1. еднозначно идентифицирана като заглавие, версия, дата, автор, номер и/или др.;
2. поддържана в актуално състояние, като се преразглежда и при необходимост сеобновява поне веднъж годишно;
3. одобрена от Директора на училището или от упълномощено от него лице;
4. класифицирана по смисъла на чл. 6 от Наредбата за минималните изисквания за мрежова и информационна сигурност;
5. достъпна само до тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения.

(3) Училището поддържа информация, доказваща по неоспорим начин изпълнението на изискванията Наредбата. Същата се поддържа в актуално състояние и 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.

Чл.13. При установяване на взаимоотношения с доставчици на стоки и услуги, които са "трети страни", Училището договаря изисквания за мрежова и информационна сигурност, включително:

1. за сигурност на информацията, свързани с достъпа на представители на трети страни до информация и активите на Училището;
2. за доказване, че третата страна също прилага адекватни мерки за мрежова и информационна сигурност, включително клаузи за доказването на прилагането на тези мерки чрез документи и/или провеждане на одити;
3. за прозрачност на веригата на доставките; третата страна трябва да е способна да 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. за 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 инцидент.

(2) Училището определя служител или служители, отговарящи за спазване на изискванията по ал. 1 и параметрите на нивото на обслужване.

(3) Училището изготвя план за действие в случай на неспазване на уговорените дейности и клаузи с третата страна.

Чл.14. С цел повишаване на квалификацията на служителите и на осведомеността им по отношение на мрежовата и информационната сигурност, настоящата политика е сведена до знанието им.

Чл.15. Потребителите на информационни системи в Обединено училище „Иван Вазов“ село Пашови са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл.16. (1) Училището извършва анализ и оценка на риска за мрежовата и информационната сигурност регулярно, 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, влизащи в обхвата на Наредбата за минималните изисквания за мрежова и информационна сигурност.

(2) Анализът и оценката на риска са документиран процес по смисъла на чл. 5, ал. 1, т.6 от Наредбата. В него са регламентирани нивата на неприемливия риск и отговорностите на лицата, участващи в отделните етапи на процеса.

(3) Анализът и оценката на риска се извършват по методика, гарантираща съизмерими, относително обективни и повтарящи се резултати. Методиката се одобрява от Директора на училището и е достъпна за лицата, на които е възложено да участват в процеса. Може да се прилага препоръчителна методика съгласно приложение № 3 от Наредбата.

(4) На основание на анализа и оценката на риска Училището изготвя план за намаляване на неприемливите рискове, който включва минимум:

1. подходящи и пропорционални мерки за смекчаване на неприемливите рискове;
2. необходими ресурси за изпълнение на тези мерки;
3. срок за прилагане на мерките;
4. отговорни лица.

Раздел II

АНАЛИЗ И ОЦЕНКА НА РИСКА ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ

Чл.17. Управлението на риска за сигурността на информационните и комуникационните системи е част от политиката за управлението на мрежовата и информационната сигурност в Обединено училище „Иван Вазов“ село Пашови. По своята същност управлението на риска представлява съвкупност от процеси за идентифициране на потенциалните заплахи към носителите на информация и активите, участващи в предоставянето на електронни услуги, анализ и оценка на рисковете, породени от тези заплахи.

Чл.18. Основните понятия, част от процеса по управление на риска са както следва:

1. конфиденциалност – свойство на информацията да не е предоставена или разкрита на неоторизирани лица (т. 2.12 ISO/IEC 27000).
2. интегритет – качество на информацията за точност и пълнота (т. 2.40 ISO/IEC 27000).
3. наличност на информация – качество да бъде достъпна и използваема при поискване от оторизирано лице (т. 2.9 ISO/IEC 27000).

Чл.19. Цел на процеса за управление на риска е Училището да минимизира загубите от потенциални нежелани събития, настъпили в резултат от реализиране на заплахи към сигурността на мрежите и информационните системи, които биха засегнали конфиденциалността, интегритета и достъпността на информацията, създавана, обработвана, предавана и унищожавана чрез тях в Училището.

Чл.20. Методиката за управление на риска има за цел да даде общ подход при анализа и оценката на риска за сигурността на информационните и комуникационните системи, предоставяни от Училището, с цел получаване на съизмерими, относително обективни и повтарящи се резултати чрез:

1. регламентиране на дейностите и тяхната последователност при анализа и оценката на риска за електронните услуги;
2. определяне на критериите;
3. определяне на приоритетите на риска.

Чл.21. Анализът и оценката на риска са част от процеса за управлението му в Училището и се обосновават на познаване на всички компоненти, имащи отношение към целите.

Чл.22. За целите на управлението на сигурността на мрежите и информационните системи е необходимо да се:

1. познават всички обекти и субекти, които участват пряко или косвено в дейностите, попадащи в обхвата на Наредбата (информационни и комуникационни системи с прилежащия им хардуер, софтуер и документация; поддържащите ги системи (електрозахранващи, климатизирани и др.); оперативни процеси/дейности; служители и външни организации), наричани за краткост "информационни активи";

2. идентифицират и анализират всички потенциални нежелани събития с тях, наричани за краткост "заплахи", които биха довели до загуба на конфиденциалност, интегритет и достъпност на електронните услуги и/или информацията в тях;
3. оценява вероятността от настъпване на тези събития, като се вземат предвид слабостите (уязвимости) на информационните активи и мерките, които са предприети за справяне с тях;
4. оценява въздействието (загуби на ресурси (време, хора и пари), неспазване на нормативни и регулаторни изисквания, накърняване на имидж, неизпълнение на стратегически и оперативни цели и др.) от евентуално настъпване на тези нежелани събития въпреки предприетите мерки;
5. оценява рискът за сигурността;
6. набелязват мерки за смекчаване на рисковете с висок приоритет.

Чл.23. При анализ и оценка на риска Училището използва регистър на рисковете (риск-регистър).

Чл.24. В риск-регистъра се нанасят всички информационни активи, имащи отношение към обхвата на Наредбата:

1. информационни системи;
2. хардуерни устройства, с които са реализирани информационните системи;
3. софтуери, с които са реализирани информационните системи;
4. бази данни, включително лични данни по смисъла на GDPR;
5. записи за събитията (логове, журнали) на информационните системи;
6. документация на информационните системи (експлоатационна и потребителска);
7. комуникационни системи;
8. хардуерни устройства, с които са реализирани комуникационните системи;
9. фърмуерът на тези устройства;
10. софтуери на комуникационните системи;
11. записи за събитията (логове, журнали);
12. документация (експлоатационна и потребителска);
13. поддържащи системи (електрозахранващи, климатични);
14. системи за контрол на физическия достъп и на околната среда;
15. процеси/дейности, свързани с управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
16. документация на тези процеси и дейности;
17. служители, имащи отговорности към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
18. външни организации, имащи отношение към управлението, експлоатацията и поддръжката на информационните и комуникационните

системи;

Чл.25. (1) За всеки от информационните активи в риск-регистъра на Училището се нанасят заплахите/нежеланите събития, които биха довели до нарушаване на конфиденциалността, интегритета и достъпността на информацията.

(2) Училището отчита всички потенциални заплахи, произтичащи вътре или извън администрацията, настъпили случайно или преднамерено, като се има предвид уязвимостта на информационния актив към съответната заплаха.

Чл.26. В риск-регистъра на Училището за всяка заплаха се вписва какви мерки са предприети срещу нея.

Чл.27. В риск-регистъра за всяка заплаха се вписва оценката за нейното въздействие – щетите (материални и нематериални), които може да причини, ако се реализира. За оценка на въздействието се използва петстепенна скала от 1 до 5, като при 1 щетите са незначителни, а при 5 са най-големи.

Чл.28 (1) Определя се вероятността за възникване на дадена заплаха, като се вземат предвид предприетите вече мерки. Колкото повече са предприетите защитни мерки, толкова по-ниска е вероятността от възникване на заплахата. При оценка на вероятността се вземат предвид следните фактори:

1. за реализиране на преднамерени заплахи: ниво на необходимите умения, леснота надостъпа, стимул и необходим ресурс;
2. за реализиране на случайни заплахи: година на производство на хардуера и софтуера, ниво на поддръжката им, квалификация на поддържащия персонал, ресорно обезпечаване на експлоатационните процеси, контрол върху тях и др.

(2) В риск-регистъра за всяка заплаха се нанася оценката за нейното въздействие.

Чл.29. За оценка на въздействието се използва петстепенна скала от 1 до 5 и като се има предвид определен период, например една година:

1. вероятността от реализирането на заплахата е под 10 %;
2. вероятността от реализиране на заплахата е от 10 % до 30 %;
3. вероятността от реализиране на заплахата е от 30 % до 50 %;
4. вероятността от реализиране на заплахата е от 50 % до 70 %;
5. вероятността от реализиране на заплахата е над 70 %.

Чл.30. За получаване на оценката на риска в Училището се използва следната формула:

(Оценка на въздействие x Оценка на вероятност) = Оценка на риска

Чл.31. С цел прилагане на пропорционални на заплахите механизми за защита в Училището се прави приоритизация на рисковете на база на тяхната оценка и

праговете, заложи в Наредбата.

Чл.32. (1) Приема се, че за рискове с приоритет 3 по смисъла на Наредбата не се изисква предприемане на допълнителни мерки за смекчаване на заплахите, които ги пораждат.

(2) За рисковете с приоритет 2 по смисъла на Наредбата се прави анализ на възможните мерки, които биха могли да се предприемат за смекчаването им, и се преценява дали разходът на ресурси за прилагането им е пропорционален на щетите от реализиране на заплахата. В случай че щетите са повече от разходите, се определят отговорно лице и срок за прилагане на тези мерки.

(3) За всички рискове с приоритет 1 се определят отговорни лица от (Касиера на Обединено училище „Иван Вазов“ село Пашови), планират се мерки, които биха намалили риска от реализиране на конкретната заплаха, и се определят срокове за прилагането им.

Чл.33. (1) Отговорните лица за съответните рискове организират прилагането на планираните мерки за защита и наблюдават инцидентите и щетите, свързани с тях. При необходимост инициират нов анализ и оценка на риска за тази заплаха.

(2) Директорът на училището организира периодично, но не по-малко от веднъж в годината, анализ и оценка на риска, както и при всяко изменение в информационната и/или комуникационната инфраструктура промяна на административната структура и функциите.

РАЗДЕЛ III

КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

Чл.34. (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, Об.У „Иван Вазов“ 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:

Категория	Описание	Примери (неизчерпателни)
Публична информация	Информация, която може да бъде обработвана и разпространявана в	(а)Финансови отчети, публикувани до обществени

	рамките на Об.У „Иван Вазов“ или извън него без никакво отрицателно въздействие върху училището, някой от неговите партньори, и/или свързани лица.	органи; (б)Информация, достъпна чрез публични ресурси или публично известна по друг начин, освен ако не е станала обществено достояние вследствие на действия на служители в нарушение на правилата за защита на информацията
Вътрешна информация	Всяка употреба на информация по какъвто и да е начин, в случай, че е извършена в нарушение на изискванията на приложимите закони или подзаконови актове, тази Политика или всяка друга регулация, приета от Об.У „Иван Вазов“ може да навреди на интересите на училището и/или нейните служители, партньори.	(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.
Поверителна информация	Всяка информация от такова значение за Об.У „Иван Вазов“, както и за 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. 35. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

- разделяне на потребителски от администраторски функции;
- установяване на нива и достъп до информация;
- регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;
- осъществяването на контрол.

Чл. 36. 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.37. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва от Системния администратор/и, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 38. 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. 39. Лицата, които обработват лични данни, използват достатъчно сложни и уникални пароли, които не се записват или съхраняват онлайн. Индивидуалните пароли не се използват съвместно с други потребители.

Чл. 40. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 41. Всички носители на лични данни се съхраняват в безопасна и сигурна среда - в съответствие със спецификациите на производителите, в заключени шкафове, с ограничен и контролиран достъп.

Чл. 42. На служителите във Об.У „Иван Вазов“- Пашови, които използват електронни бази данни и техни производни (текстове, разпечатки) се забранява:

- (1) да ги изнасят под каквато и да е форма извън служебните помещения;
- (2) да ги използват извън рамките на служебните си задължения;
- (3) да ги предоставят на външни лица без да е заявена услуга.

Чл. 43. 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. 44. При изнасяне на носители извън физическите граници на Об.У „Иван Вазов“ с. Пашови, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 45. 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. 46. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до зловреден софтуер. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл. 47. 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 след това цялата информация е изтрита от тях преди унищожаване.

Чл. 48. Събирането, подготовката и въвеждането на данни на интернет страницата се извършва от оправомощени служители на Об.У „Иван Вазов“ село Пашови. Длъжностните лица притежават потребителски имена и пароли за актуализиране на сайта.

Чл. 49. Събирането и подготовката на данните се извършва от служителите, след което данните се предават в електронен вид (на файлове) на служителите отговорни за качването им на интернет страницата на училището.

РАЗДЕЛ IV РАБОТНО МЯСТО

Чл. 50. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 51. Работното място се оборудва при спазване на изискванията на Наредба № 7 от 15.08.2005 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи (Издадена от министъра на труда и социалната политика и министъра на здравеопазването, обн., ДВ, бр. 70 от 26.08.2005 г.).

Чл. 52. Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения съобразно изискванията на Приложение № 11 към чл. 45 ал. 2 от Наредба за общите изисквания за оперативна съвместимост и информационна сигурност (Приета с ПМС № 279 от 17.11.2008 г. - изм. и доп. ДВ. бр. 48 от 31.05.2013г.).

Чл. 53. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място или ползвани от него на сървъра на локалната компютърна мрежа съобразно дадените му права.

Чл. 54. 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. 55. Забранява се на външни лица работата с персоналните компютри на Об.У „Иван Вазов“ с. Пашови, 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 Системния администратор.

Чл. 56. След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off.

Чл. 57. При загуба на данни или информация от служебния компютър, служителят

незабавно уведомява прекия си ръководител и Системния администратор, който му оказва съответна техническа помощ.

Чл. 58. 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. 59. Инсталиране и размястване 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 Системния администратор.

Чл. 60. 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 Об.У „Иван Вазов“ село Пашови.

Чл. 61. 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. 62. 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 неоторизиран достъп.

Чл. 63. Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до Системния администратор.

Чл. 64. 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, факсовете, 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.

РАЗДЕЛ V

ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 65. Системният администратор извършва необходимите настройки за достъп до локалната мрежа (DC) и интернет като създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща във Об.У „Иван Вазов“ село Пашови.

Чл. 66. Ползването на компютърната мрежа и електронна поща от служителите става чрез получените потребителско име и парола.

Чл. 67. 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. 68. 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. 69. Компютрите, свързани в мрежата на училището използват интернет само от доставчици, с които Об. У „Иван Вазов“ село Пашови има сключен договор за доставка на интернет.

Чл. 70. Забранява се свързването на компютри едновременно в мрежата на Об.У „Иван Вазов“ село Пашови и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на Об.У „Иван Вазов“ село Пашови и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и Наредба за общите изисквания за оперативна съвместимост и информационна сигурност (Загл. изм. - ДВ, бр. 5 от 2017 г., в сила от 01.03.2017 г.).

Чл. 71. Забранява се инсталирането и използването на комуникатори (като icq, skype, социални мрежи и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на Об.У „Иван Вазов“ село Пашови 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 Об.У „Иван Вазов“ с. Пашови.

Чл. 72. Забранява се съхраняването на сървърите на Об.У „Иван Вазов“ на лични файлове с текст, изображения, видео и аудио.

Чл. 73. 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 VI

ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 74. С цел антивирусна защита се прилагат следните мерки:

- (1) Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.
- (2) Системният администратор 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 системата;
 - 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 работна станция, всеки служител от съответното работно място задължително информира Системния администратор и прекия ръководител.

РАЗДЕЛ VII

НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 75. Следните мерки се прилагат с цел антивирусна защита:

1. Всички сървъри и устройства за съхранение на данни са свързани към устройства за непрекъсваемост на ел. захранването.
2. При липса на ел. захранване за повече от 10 мин., Системният администратор започва процедура по поетапно спиране на сървърите.
3. При срыв в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация. При възстановяване на мрежата, всички локално запазени файлове следва да се преместят отново на сървър и да се изтрият локалните копия.

РАЗДЕЛ VIII

СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 76. Осигурява се автоматизирано създаване на резервни копия на всички бази данни и електронни документи.

Чл. 77. Информацията, включително тази, съдържаща лични данни, се резервира по следния начин:

- (1) Автоматизирано и планово се извършва архивиране на цялата работна информация на сървърите и дисковите масиви;
- (2) Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг сървър/компютър и да се продължи работният процес без чувствителна загуба на данни;
- (3) Архивирането на базите данни се извършва съгласно Процедури за архивиране и възстановяване на данни във Об.У „Иван Вазов“ село Пашови утвърдени със Заповед на Директора на училището.

РАЗДЕЛ IX

УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Чл. 78. Изявяват се необходимите ресурси и се използват по организиран начин за противодействие на отрицателно въздействащи събития, свързани с надеждността и сигурността на информационните активи. Такива въздействия могат да са резултат от

атаки, вируси и друг злонамерен код, опити за проникване и отказ от услуги, неразрешен достъп до или некоректно ползване на информационно-технологичните системи и данни и др.

Чл. 79. Дейности, свързани с работа по инцидентите:

- (1) Пробивите в сигурността на информацията се докладват от всеки служител на прекия ръководител;
- (2) Работата по инцидентите се извършва от упълномощени за това служители, притежаващи необходимата подготовка и опит;
- (3) Инцидентите и предприетите действия се записват и документират в „Регистър на инцидентите по сигурността“.
- (4) Отстраняване на последствията от инцидента възможно най-бързо.

РАЗДЕЛ X

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Служителите на Обединено училище „Иван Вазов“ село Пашови са длъжни да познават и спазват разпоредбите на настоящата Политика.

§ 2. Контролът по спазване на правилата се осъществява от Директора на училището или Упълномощено със Заповед лице.

§ 3. Настоящата политика се разглежда и оценява периодично с оглед ефективността ѝ, като Об.У „Иван Вазов“ с. Пашови може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Политиката е разработена съгласно Наредбата за минимални изисквания за мрежова и информационна сигурност (приета с ПМС № 186 от 19.07.2019 г. и обнародвана в ДВ, бр. 59 от 26.07.2019 г.) , изискванията на ЗЕУ, Закона за Киберсигурност и е утвърдена със Заповед №519-80 /15 .09.2021г. на Директора на училището.