

Основно училище
гр. Варна, район Аспарухово
ул. „Кирил и Методий“ №8



„Христо Ботев“
тел. 052/370 696; 0877/446 812
e-mail: info-400026@edu.mon.bg

Х

Виктория Шереметова

Директор

Утвърдил:
ВИКТОРИЯ ШЕРЕМЕТОВА
Директор на ОУ „Христо Ботев“

Правила за мрежова и информационна сигурност

на ОУ „Христо Ботев“ – гр. Варна

/утвърдени със заповед № РД-09-72/16.09.2024 г./



Съдържание:

Въведение.....	5
Свързани документи:	5
Списък на разпространение.	5
1. Цел и обхват на документа.	6
1.1. Цел.	6
1.2. Обхват.....	6
1.3. Отговорности.	6
2. Общи положения.	7
2.1. Стандарти, основни указания и модели, приети от организацията.	7
2.2. Формат и обхват на договорните отношения.	7
3. Определяне на обхвата на СУИС.	7
4. Основни принципи на СУИС:	7
4.1. Оценка и управление на риска:	7
4.2. Управление на информационните активи на ОУ „Христо Ботев“ – гр. Варна.	8
4.2.1. Законови и регулаторни изисквания.....	9
4.2.2. Допустима употреба.....	10
4.2.3. Правила за информационна сигурност.....	10
4.2.4. Техническо осигуряване на компютърна и периферна техника за служителите на ОУ „Христо Ботев“ – гр. Варна:	10
4.2.5. Електронна поща и чат:	11
4.2.6. Контакт с групи със специален интерес.....	12
4.2.7. Зловреден софтуер и вируси.....	12
4.2.8. Използване на Интернет.	12
4.2.9. Забранена употреба:	13
4.2.10. Бази данни.	14
4.2.11. Защита на софтуер и фърмуер; копиране и инсталиране на софтуер на информационни активи на ОУ „Христо Ботев“ – гр. Варна:	14
4.2.12. Комуникация:.....	15
4.2.13. Конфиденциалност:.....	15
4.2.14. Генериране на логове и мониторинг:	15
4.2.15. Сигурност.	16



4.2.16.	Онлайн трансакции.	16
4.2.17.	Право на интелектуална собственост - включително авторски права.	17
4.2.18.	Мрежови и локални дискове:	17
4.2.19.	Съхранение на записи:	17
4.2.20.	Достъп:	18
4.2.21.	При използване на лично устройство.	18
4.2.22.	Указания към мобилните устройства:	18
4.2.23.	Безжичен достъп в рамките на работните помещения:	19
4.2.24.	Архивиране и възстановяване на файлове.	19
4.2.25.	Предаване, регистрация, отчетност и съхраняване на приетите документи в учрежденския архив:	19
	Съгласно Вътрешни правила за дейността на учрежденския архив в ОУ „Христо Ботев“ – гр. Варна.....	19
4.2.26.	Ред за достъп и ползване на архива на ОУ „Христо Ботев“ – гр. Варна:.....	19
	Достъп до архивохранилището има само длъжностното лице, отговарящо за съхранението и използването на документите от архива, а в негово отсъствие – лица оторизирани да извършват контрол по опазването и съхраняването на документите.....	19
4.2.27.	Унищожаване на информационни активи на хартиен носител.....	19
4.2.28.	Изваждане от употреба и унищожаване на ИТ оборудване:	19
4.2.29.	Връщане на активи.	20
4.3.	Управление на сигурността на човешките ресурси. Подбор на кадри. Срокове и условия за наемане на работа.	20
4.3.2.	Подбор на кадри:	21
в)	Обучение.	21
	Процедура за обучение на персонала се извършва по „Основни процедури и работни инструкции описващи процесите при управление на човешките ресурси в ОУ „Христо Ботев“ – гр. Варна“, Приложение №9 Работна инструкция „Планиране и организиране на обучението на персонала“.	21
4.4.	Сигурност на инфраструктурата.	21
4.5.	Физическа сигурност.....	25
5.	Ангажираност на ръководството.	26
6.	Съответствие, контрол и преглед.....	26
	Приложение А - Процес при назначаване/напускане на служител, разпределение на задължения	27
	Приложение Б - Функции на служителят, отговарящ за мрежовата и информационната сигурност.....	28

Основно училище
гр. Варна, район Аспарухово
ул. „Кирил и Методий“ №8



„Христо Ботев“
тел. 052/370 696; 0877/446 812
e-mail: info-400026@edu.mon.bg

Приложение В - Декларация на служителя 29
Приложение Г - Уведомление за инцидент свързан с информационната сигурност..... 30



Въведение.

Информацията, в качеството си на най-важния ресурс на ОУ „Христо Ботев“ – гр. Варна, може да бъде определена като актив, който има висока стойност. С цел предотвратяване на рискове, които могат да доведат до правни, финансови, регулаторни, оперативни и други последствия, стойността на тази информация следва да бъде запазена.

В училището се акумулира голямо количество чувствителна информация, в това число информация за служители, директори и външни лица, ученици, продукти, услуги и финанси. Голяма част от тази информация се събира, обработва и съхранява в електронна форма, поради което компютърната сигурност и информационната защита на компютърните системи и мрежи и използваната в тях информация са едни от основните елементи, за които се прилага информационната сигурност.

Правилата за мрежова и информационна сигурност са основен документ във връзка с осигуряване на защита на информационните активи без значение дали те са физически – на хартиен носител или под формата на цифрови масиви, както и основен документ на училището, представящ управленската стратегия за сигурността.

Те представляват рамка за дефиниране на уместно поведение, определяне на необходимите средства, избор на подходящите контроли и създаването на необходимите политики, процедури, инструкции, ръководства и т.н.

Правилата за мрежова и информационна сигурност на ОУ „Христо Ботев“ – гр. Варна акцентират върху трите ключови аспекта на информационната сигурност, а именно:

- Наличност – необходимата информация да бъде налична всеки път, когато даден процес я изисква;
- Цялостност – информацията да бъде непроменена, а във вида, в който е записана;
- Поверителност – достъпът до съответната информация да бъде подсигурен по начин, който с максимална точност да идентифицира потребителя, достъпващ тази информация.

Свързани документи:

- Опис на информационните активи;
- Физическа схема на свързаност;
- Логическа схема на информационните потоци;
- Документация на структурната кабелна система;
- Политика за класификация на информацията;
- Ръководство за управление на риска;
- Оценка на риска на информационните активи и план за третиране на риска;
- План за действие при киберинциденти, за връщане на системите в предишното им състояние и за техническа профилактика на устройствата;

Списък на разпространение.

Настоящият документ и всички негови актуализации следва да бъдат разпространявани до:

- (1) Всички служители на ОУ „Христо Ботев“ – гр. Варна;
- (2) Регионално управление на образованието – гр. Варна.



1. Цел и обхват на документа.

1.1. Цел.

Настоящите правила имат за цел:

- Да дефинират основните изисквания към Системата за управление на информационната сигурност (СУИС) на ОУ „Христо Ботев“ – гр. Варна;
- Да осигурят адекватна защита на конфиденциалността, целостта и достъпността на информационните активи на училището.

1.2. Обхват.

Правилата обхващат процесите в ОУ „Христо Ботев“ – гр. Варна, отговорности и ангажименти на ръководството, както и поддържане на СУИС.

1.3. Отговорности.

1.3.1. Настоящите правила се прилагат от всички служители на училището.

1.3.2. Директорът на училището:

- а) отговаря за мрежовата и информационна сигурност, дори когато дейността е възложена за изпълнение на трети страни;
- б) взема необходимите документирани решения чрез утвърждаването на правила, процедури и други, както и чрез осигуряване на необходимите ресурси и инфраструктура за гарантиране на мрежовата и информационна сигурност на използваните информационни активи, мрежи и системи.
- в) Разпределя правата за използване на информационните системи и ролите и отговорностите, свързани с опазване на информационните активи и сигурността на информацията;
- г) Координира прилагането на мерки за осигуряване на информационна сигурност;
- д) Организира оценяване на потребностите и планира необходимите ресурси за осигуряване на информационната сигурност;
- е) Утвърждава цялата допълнителна документация свързана с мрежовата и информационна сигурност;
- ж) Организира проверки за оценяване степента на постигнатата мрежова и информационна сигурност.

1.3.3. Определеното, със заповед от директора лице, отговарящо за мрежовата и информационна сигурност, упражнява контрол по изпълнение на мерките от системата за управление на информационната сигурност (СУИС).

1.3.4. Ръководството и лицето, отговорно за мрежовата и информационна сигурност, изискват от служителите и доставчиците да прилагат мерките за сигурност в съответствие с установените правила и процедури на СУИС, внедрени в училището.

1.3.5. Отговорностите на служителите за гарантиране на мрежовата и информационна сигурност на използваните информационни мрежи и системи се определят в длъжностните им характеристики, в настоящите правила за мрежова и информационна сигурност, работни планове, заповеди, както и на друго документирано основание.



2. Общи положения.

2.1. Стандарти, основни указания и модели, приети от организацията.

В училището е внедрена система за видеонаблюдение.

2.2. Формат и обхват на договорните отношения.

В рамките на обхвата на СУИС на ОУ „ХРИСТО БОТЕВ“ се поддържат взаимоотношения с лица и организации, като втора или трета страна. Договорните отношения с външните организации се базират на проведени процедури, съответстващи на изискванията на законово или подзаконово определени правила за провеждането им.

3. Определяне на обхвата на СУИС.

За да установи нейния обхват, училището определя границите и приложимостта на системата за управление на сигурността на информацията, както следва:

(1) Процеси: Всички дейности, попадащи в обхвата на ангажиментите на ОУ „Христо Ботев“ – гр. Варна.

(2) Физически граници:

СУИС обхваща следните сгради на ОУ „Христо Ботев“ – гр. Варна

1. гр. Варна, ул. „Кирил и Методий“ № 8

Логически блок схеми:

- Схеми на LAN мрежа;
- Логическа схема;
- Блок схема на пожароизвестителна система.

4. Основни принципи на СУИС:

4.1. Оценка и управление на риска:

а) Целта на управлението на риска по сигурността на информацията е да идентифицира стойности и управлява рисковете, свързани с информационната сигурност, тяхната вероятност и потенциално въздействие върху дейностите и стратегията на училището.

Управлението на риска по сигурността на информацията се осъществява непрекъснато, включително и при въвеждането в експлоатация на нови процеси или при промяната на съществуващите такива, за да бъдат избегнати външни и/или вътрешни заплахи.

б) Отговорностите, свързани с управлението на рисковете при информационната сигурност, като част от цялостното управление на риска в училището, са ясно разпределени и адекватно обсъдени с всички служители. Отговорностите спрямо всяка група рискове, свързани с информационната сигурност, са определени в настоящия документ и в свързаните с него нормативни документи, част от СУИС на училището.

в) В училището се изпълнява процес по годишна оценка на риска, която да идентифицира основните стратегически развития в сферата на информационните технологии, възникващи заплахи и уязвими места или когато се налагат съществени изменения в целите, вътрешните и външните условия на работа, информационната и комуникационната инфраструктура, дейностите или процесите. Резултатите от тази годишна оценка на риска се отразяват в Доклад за оценка на риска, в който са регламентирани нивата на неприемливия риск и отговорностите на лицата, участващи в отделните етапи на процеса.



г) Анализът и оценката на риска се извършват по методика, гарантираща съизмерими, относително обективни и повтарящи се резултати. Методиката се одобрява от директора на училището, като може да се прилага препоръчителна методика съгласно приложение № 3 от Наредба за минималните изисквания за мрежова и информационна сигурност.

д) Процесът на управление на риска включва минимум следните етапи:

1. идентификация на информационните активи;
2. идентифициране на заплахите за всеки от информационните активи;
3. оценка на въздействието на всяка заплаха спрямо щетите, които може да причини, ако се реализира;
4. оценка на вероятността за възникване на всяка заплаха;
5. оценка на рисковете;
6. приоритизация на рисковете;
7. смекчаване на рисковете;
8. избор на защитни мерки и отговорни лица и срокове за прилагането им;
9. реализация и проверка на избраните мерки;
10. оценка на резултативния риск.

е) На основание на анализа и оценката на риска се изготвя план за намаляване на неприемливите рискове, който да 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.

ж) В училището се събират данни и извършва анализ на вида и броя на инцидентите, както и на направените разходи по разрешаването им, с цел да се идентифицират повтарящите се или тези с голямо влияние, да се ограничат честотата, щетите и загубите от появата им в бъдеще.

4.2. Управление на информационните активи на ОУ „Христо Ботев“ – гр. Варна.

а) Активите включват информация, софтуер и физически ресурси.

Базата данни, включваща информационните активи на училището, следва да бъде поддържана и обновявана непрекъснато, за да осигурява актуална информация за текущите и/или нови типове на данните. Технологичните активи на училището следва да се използват от служителите само за служебни цели и в съответствие с установените правила за сигурност. Политиката за класификация на информацията определя съответните изисквания за защита срещу различни типове рискове, свързани с данните по време на целия им жизнен цикъл (от създаването им до тяхното унищожаване).

б) Всеки информационен актив на училището следва да бъде описан в база данни с цел разрешаването на инциденти, анализ и оценка на риска, управление на уязвимости и управление на измененията. Описът следва да съдържа информация като:

- еднозначна идентификация, като инвентарен, сериен номер или др.;
- основни характеристики;
- услуги, процеси и дейности, в които участва;
- местоположение;
- година на производство, където е приложимо;



- дата на въвеждане в експлоатация, където е приложимо;
- версия, където е приложимо;
- местонахождение на свързаната с него документация (техническа, експлоатационна, потребителска и др.);
- отговорно лице.

в) Отговорник на актива е служител на училището, определен със заповед, на когото ръководството възлага следните отговорности:

- правилно да съхранява поверените му активи;
- да съдейства при категоризирането на активите и да следи за това те да бъдат съхранявани съобразно направената категоризация;
- да извършва периодичен преглед на ограниченията за достъп до активите и на категоризирането им;
- да участва при извършването на оценка и преоценка на риска за поверените му активи.

г) Определеният отговорник няма фактически права на собственост или разпореждане върху управляваните от него активи на училището, с изключение на тези, които са пряко свързани с неговата персонална квалификация – дипломи, сертификати, удостоверения.

д) Информационните активи се съхраняват както електронно, така и на хартиен носител. Електронните носители подлежат на износване, стареене и подмяна, поради което правилното изваждане от употреба и сигурно унищожаване е задължително за сигурността на информацията и опазването на околната среда.

Всички електронни писма и важни съобщения, които имат отношение към дейността на училището, се представят за завеждане с входящ номер в деловодната система от определеното длъжностно лице.

Всички електронни носители като твърди дискове, USB устройства, CD/DVD дискове и други трябва да бъдат надлежно изтрети преди тяхното отчисляване и бракуване, съгласно процесите описани в настоящите правила, със специализирани програмни продукти за сигурно изтриване на данните, защото при стандартното изтриване на файлове или форматиране на дискове, данните все още са достъпни със специализирани софтуерни средства.

Всички носители, които не позволяват изтриване на данните от тях (като хартиени носители, CD, DVD и т.н.), следва да бъдат надлежно унищожени от специализирани устройства тип „шредер“ и др.

4.2.1. Законови и регулаторни изисквания.

Служителите трябва да спазват стандартите и добрите практики за конфиденциалност, опазване и наличност на данните, и цялостност при употребата на информационни системи на МОН и на училището за съхранение, възпроизвеждане, достъп и разпространение на информация.

Служителите са задължени да:

- не достъпват, свалят или съхраняват неподходящо или забранено съдържание;



- не запазват софтуер, който не е приет за допустим за работа в училището, съгласно утвърден списък или големи лични файлове на мрежови или локални дискови устройства на МОН или училището;
- се уверят, че личната кореспонденция и дейности не са в конфликт със служебни задължения;

Когато служителите имат необходимост да получат достъп до ресурси, които са забранени по смисъла на тази политика, те трябва да потърсят и получат необходимото разрешение от директора и лицето отговорно за МИС в училището.

4.2.2. Допустима употреба.

Използването на активи на училището за лични цели от служителите да се сведе до минимум и да става след разрешение.

Неправилното и неподходящо използване на активи на МОН и/или на училището е забранено.

4.2.3. Правила за информационна сигурност.

Всички служители трябва да се запознаят със своите роли и отговорности, наложени от правилата за информационна сигурност на училището.

Директорът или определено от него лице да предостави списък с приложимите правила на служителите, включително и на новоназначените.

Всеки служител трябва да подпише декларацията в приложение „В“ от този документ, с която да удостовери, че е запознат и разбира своята роля и отговорност по смисъла на тези правила за информационна сигурност, и при неизпълнение носи дисциплинарна отговорност.

4.2.4. Техническо осигуряване на компютърна и периферна техника за служителите на ОУ „Христо Ботев“ – гр. Варна:

а) Видът и техническите параметри на необходимата компютърна конфигурация се определя от определено със заповед лице и се одобрява от директора на училището.

б) Ремонти, подмяна на части, добавяне на компоненти или друг вид подобряване на компютърните конфигурации се извършват единствено в присъствието на определеното със заповед лице.

в) Инсталирането на компютърните конфигурации, системните и приложните програми, както и следващи промени в тях се извършват от определено със заповед лице или от упълномощените за това фирми – доставчици на компютърна, периферна техника и програмни продукти, но в присъствие на определеното със заповед лице

г) Гаранционното обслужване на техниката се извършва само от упълномощените за това сервизи.

д) Техническото обслужване (поддръжка), доколкото това не изисква намеса на сервизни специалисти, се извършва от определено със заповед лице. При необходимост от извънгаранционен ремонт лицето да се свърже със специализиран сервиз, който да извърши ремонтните дейности.

е) Компютърната и периферна техника, която не се използва, да се предава на определено със заповед лице за съхранение, до нейното предаване на друга институция, в случай, че може да бъде повторно използвана, или до нейното унищожаване съгласно утвърдените в настоящите правила за сигурно изваждане от употреба на ИТ активи.



ж) След края на работния ден всеки служител задължително изключва компютърната техника, на която работи, или я привежда в режим log off/lock.

з) Копирната, принтерна и друга техника, предоставена на служителите в училището, да се използва само за служебни цели.

и) Не се допуска:

1. Самостоятелни опити за поправка на принтерна, копирна и друга техника. При съмнение за съществуващ проблем служителите следва да информират определеното със заповед лице.

2. Работа на външни лица с наличната копирна, принтерна и друга техника, както и техни опити за отстраняване на възникнали проблеми, освен на лица - служители на оторизираните за това фирми, да става след заявка от страна на определеното със заповед лице.

3. Смяната на тонер касети отстраняването на заседнали листа да се извършва само от обучени за това служители.

4.2.5. Електронна поща и чат:

а) Служителят трябва да:

- се увери, че личната кореспонденция не е в конфликт със служебните задължения и когато е възможно да ограничава подобна кореспонденция за часовете извън работно време;
- не използва личната кореспонденция, която е в конфликт със служебните задължения (не съдейства за изпълнение на служебните задължения) в работно време;
- се увери, че не пречи на работата на други служители или не блокира ресурси, необходими за изпълнението на служебни задачи;
- поне веднъж месечно да почиства пощенската си кутия от лични и ненужни съобщения;

б) Служителите не трябва да отговарят на спам или на масово изпращани непоискани търговски съобщения, при никакви обстоятелства. Ако в съобщението по електронната поща има изпратен линк, служителят следва първо да го копира и провери (без да натиска върху него) на сайт за сканиране за зловреден код (напр. <https://www.virustotal.com/>).

в) Служителят трябва да подхожда с изключително внимание при отварянето на прикачени файлове, особено ако имейлът е изпратен от непознат, като обръща особено внимание на конкретното описание в полето „From“.

г) В случай на съмнения, служителят не трябва в никакъв случай да отваря линкове/хипервръзки в съмнителни съобщения получени по електронната поща, без да се консултира със служителя отговорен за МИС в училището.

д) Неоторизирани масови имейли не са разрешени. Служителят трябва да внимава при изпращането на чувствителна информация до лица извън мрежата на МОН, РУО – Варна и училището. Ако е необходимо да се изпрати чувствителна информация, тя трябва да бъде криптирана или защитена с парола.

е) Служителят има право и задължение да докладва съобщения (различни от спам) с обиден, унижителен или заплашителен характер, които смята, че са изпратени умишлено. Всички сигнали ще се третират безпристрастно, конфиденциално и своевременно. Служителят да адресира своите сигнали до директор и/или определено със заповед лице.



ж) Всяко неетично и незаконно използване на ИТ системите на МОН или на училището може да доведе до незабавно прекратяване на достъпа, дисциплинарни и съдебни мерки.

4.2.6. Контакт с групи със специален интерес.

Ръководството на училището разрешава на компетентни служители да поддържат регламентирани контакти с групи по интереси, форуми на специалисти по сигурността или други професионални сдружения.

Посочените служители поддържат тези контакти с цел:

- достъп до най-добрите практики и получаване на актуална информация по въпросите на ИС;
- получаване на ранни предупреждения за заплахи, отнасящи се до атаки и уязвимости;
- достъп до съвети на водещи специалисти за справяне с инциденти по информационната сигурност.

4.2.7. Зловреден софтуер и вируси.

С цел предпазване от вируси или друг зловреден софтуер свалянето на файлове да се извършва само от известни и надеждни източници. Да не се зарежда (сваля) софтуер от непроверен уебсайт.

Ако служителите подозират, че компютърът им е заразен с вирус (ако работи много бавно или се държи нестабилно) трябва незабавно да стартират сканиране на компютъра с интегрираната антивирусна защита и да се свържат с отговорника за мрежова и информационна сигурност.

Използването (отварянето) на изтеглени файлове от Интернет пространството (сайтове, лични пощи, форуми, чат-програми и др.) във връзка с изпълнение на служебните задължения, става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, служителите незабавно се обръщат към отговорника за мрежова и информационна сигурност, който от своя страна предприема действие по документирани и отстраняване или привеждане в безопасна среда за анализ на зловредния код.

В случай на Ransomware атака (процес при който се криптират част или всички файлове на заразената компютърна техника и се визуализира съобщение за откуп), компютърната техника незабавно се изключва от мрежовите ресурси на училището, след което се проверяват всички налични компютърни конфигурации за наличие на зловреден код. В случай, че се установят заразени компютърни конфигурации, те не се рестартират или изключват. Плащането на откуп за декриптиране на информацията е строго забранено.

За инцидентите се уведомява длъжностното лице по мрежова и информационна сигурност в РУО – Варна.

4.2.8. Използване на Интернет.

Сърфиране в мрежата, което не е свързано с изпълнение на служебните задължения през работно време, е забранено.

а) Служителят не следва да достъпва през работно време:

1. онлайн стрийминг сайтове (радио, музика и видео), освен ако достъпът не е необходим за изпълнението на служебните задължения;



2. публикации в лични блогове или уебстраници, освен, ако не е свързано с естеството на работата;
3. да извършва лични бизнес трансакции (включително достъп до eBay или подобни, борсова търговия и др.);
4. Порнографски сайтове, снимки или текстове;
5. Сайтове, видео или статии, които разпространяват омраза;
6. Сайтове свързани с хакерско съдържание;
7. Сайтове за хазарт или каквито и да е нелегални и незаконни сайтове.

б) Разрешено е, ако това не пречи на изпълнението на служебните задължения:

1. участие в свързани с работа по дискуссионни групи;
2. онлайн платформи за групова учебна дейност;
3. уебсайтове за обучение и самообучение;
4. споделяне на видео и аудио уроци;
5. подготовка за представителни и състезателни дейности.

в) Компютрите, свързани в мрежата на училището използват Интернет от доставчик Ламат ООД (Аспарухово Нет) и А1 България ЕАД, с които има сключени договори.

г) При използването на информационни системи, служителите не трябва да използват опциите за запаметяване на паролите, предоставяна от браузърите.

4.2.9. Забранена употреба:

а) Служителят не трябва да създава, изпраща или достъпва информация, която може да урони репутацията на институция или личност, има подвеждащ или измамен характер, може да доведе до насилие или тормоз, представлява криминално деяние или нарушение на гражданските права, или може да доведе до обиден, нецензурен или клеветнически резултат.

б) Информацията по горната точка включва порнография или други незаконни материали. При установяване притежанието на материали, свързани с детска порнография е престъпление и отговорните ръководители са задължени да докладват на властите. Преносът, съхранението или свалянето на нецензурни или незаконни материали и съдържание, излагат служителите на риск от нарушение на законите за защита от дискриминация.

в) В допълнение към забраненото съдържание, има категория означена като неподходяща за достъпване през ИТ системите на училището. Там влизат следните категории уебсайтове:

- Порнография;
- Хазарт;
- Чат стаи;
- Онлайн запознанства;
- Престъпност/тероризъм;
- Насилие/нежелателно поведение;
- Зловреден софтуер;
- Списък със сайтове, блокирани от правителството (нелегални сайтове).



4.2.10. Бази данни.

4.2.10.1. Служителите, които използват или имат достъп до бази данни и техните производни (текстове, разпечатки, карти и скици или др. подобни), в рамките на осъществяваните от тях служебни правоотношения нямат право:

- а) Да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга);
- б) Да ги използват извън рамките на служебните си задължения;
- в) Да ги предоставят на външни лица без да е заявена услуга;
- г) Да разпространяват получената от тези бази данни информация, касаеща:
 - Данни за личността;
 - Данни за собствеността на гражданите;
 - Данни за данъчните и други финансови задължения на гражданите;
 - Данни за училището, които представляват служебна тайна и биха застрашили неговата сигурност.

4.2.10.2. Служителите, които въвеждат и актуализират електронни бази данни са длъжни да ги поддържат в актуално състояние.

Всички действия по подготовката на данни за въвеждане в информационна система, а именно: събиране, актуализиране, сортиране и подреждане се извършват съобразно вътрешните правила на училището.

Актуализацията и корекцията на електронни бази данни се извършват от съответните служители при спазване на определените права за достъп.

Форматите на електронните бази данни се определят съобразно нормативните актове и стандарти в тази област. Служителите, извършващи въвеждане и актуализация на данните, носят пълна отговорност за тяхната достоверност.

4.2.10.3. 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.

4.2.11. Защита на софтуер и фърмуер; копиране и инсталиране на софтуер на информационни активи на ОУ „Христо Ботев“ – гр. Варна:

а) Софтуер от всякакъв тип не трябва да бъде копиран или инсталиран на компютърните конфигурации на училището, освен ако съответният служител няма изрично разрешение да извършва тези дейности от директор и/или друго определено лице. Това е приложимо за всякакъв софтуер, включително софтуер, който е собственост на служителя, придобит по Интернет или чрез преносими медии като CDs/DVDs и USB дискове.

б) В училището се инсталират и поддържат само версии на използвания в системите му софтуер и фърмуер, които се поддържат от доставчиците или производителите и са актуални от гледна точка на сигурността.

в) Директорът на училището одобрява списък на софтуера, който се използва в информационните и комуникационните системи.

г) Не се допуска инсталирането и използването на софтуер и фърмуер, който не е одобрен по надлежния ред.

д) Определено със заповед лице осъществява постоянен контрол върху използвания софтуер и фърмуер, включително неговата актуалност.



е) Ако даден служител има необходимост да инсталира софтуер, утвърден в списъка за допустим софтуер, той трябва да се свърже с определеното лице.

ж) Софтуерът, който се използва от училището и не е със свободен лиценз за организации, трябва да бъде закупен, така че да се гарантира и поддържа пълната документация за него, от която да може да се установят каналите за придобиването му, кога е регистриран, кога е актуализиран и друга подобна информация.

з) Училището поддържа библиотека с дистрибутиви на използвания софтуер и фърмуер с цел намаляване на времето за възстановяване на дадена система след срив.

и) При разработване на нови или промяна на съществуващи софтуерни продукти за целите на училището, в договорите за разработка се включват ясни клаузи, гарантиращи, че правата за интелектуалната собственост остават за институцията.

4.2.12. Комуникация:

а) Всеки служител, който инициира измама, незаконни действия или злоупотреба ще бъде обект на дисциплинарни мерки и наказателно преследване.

б) Служителят носи лична отговорност, ако съдейства на лица, които дискриминират, тормозят или клеветят колеги.

4.2.13. Конфиденциалност:

а) Служителят трябва:

- Да знае, че неотроризираното разкриване на чувствителна информация е нарушение на политиките на МОН и училището, което може да представлява нарушение на закона;

- да прилага стандарти, практики и изисквания за конфиденциалност, цялостност и наличност при съхранението, възпроизвеждането, достъпа и разпространението на информация.

Съхранението на чувствителна информация в електронен вид (пренос на информация на диск или друго преносимо устройство за съхранение) означава, че устройството трябва да се третира със същото внимание, като категоризиран чувствителен файл. Да се обръща изключително внимание на употребата на електронната поща при тези обстоятелства, за да се избегне неразрешеното публикуване на чувствителна официална информация.

б) Забранява се достъпа до компютърните файлове на други служители без разрешение, което се дава от съответния потребител, собственик на информацията или от директора на училището, при наличието на основателна причина за изпълнение на служебните задължения.

4.2.14. Генериране на логове и мониторинг:

а) Училището контролира употребата на активи и ИТ системи от своите служители чрез:

1. поддържане на логове, резервни копия и архиви от работни станции, преносими компютри, сървъри, принтери и мрежови устройства, включително мобилни телефони, таблети и други ИТ системи;
2. наблюдение на работата и съхранение на логове от имейл сървъри, включително получени и изпратени имейли;



3. съхранение на логове, резервни копия (бекъп) и архиви с информация за достъпа до Интернет и употребата на мрежата.

в) При необходимост определените лица по МИС в училището следва да имат права на достъп до логовете на всеки служител, включително:

1. резервни копия и архиви на всички файлове, включително текущи и изтрити имейли;
2. имейл съобщения и прикачени файлове;
3. посетени сайтове, дата, час и продължителност на посещенията.

г) Определените лица по МИС в училището, в сътрудничество с ръководството, може да оторизират достъп до потребителски логове, когато има заплаха за:

1. Информационната сигурност на училището;
2. Личното пространство и данни на персонала;
3. Личното пространство и данни на учениците;
4. Проблеми от правно естество за училището.

4.2.15. Сигурност.

Някои от мерките за защита на комуникацията и ИТ системите на училището включват:

1. използване на пароли или ПИН на всички мобилни устройства (включително преносими компютри, телефони и PDA), които могат да бъдат откраднати;
2. за официална служебна кореспонденция и комуникация да се използва само служебната електронна поща в edu.mon.bg (info-400026@edu.mon.bg);
3. да не се използват лични имейли за изпращане на информация, както и такива от доставчици на безплатни услуги за електронни пощи (напр. abv.bg, mail.bg, yahoo.com и др.), освен при извънредни обстоятелства, и в случай че са изчерпани всички възможни сценарии за използване на служебната електронна поща в edu.mon.bg (info-400026@edu.mon.bg);
4. да не се свалят, инсталират и използват програми по сигурността, които разкриват слаби места на дадена система, освен от длъжностните лица по МИС на МОН/РУО – Варна/ училището в рамките на изпълнение на служебните им задължения;
5. да се заключват компютрите, когато не се използват. Ако компютърът е споделен, служителите задължително трябва да излизат от профила си, преди да напуснат работното място;
6. в никакъв случай да не се използват пароли от устройства на МОН/РУО - Варна или училището, за достъп до външни системи, особено Интернет сайтове.

4.2.16. Онлайн трансакции.

Служителите трябва да се уверят, че съществува подходяща степен на сигурност за всяка трансакция, засягаща договорни отношения, осъществявана чрез Интернет, която те изпълняват в хода на тяхната работа.

При онлайн покупки за служебни цели служителят трябва да обърне необходимото внимание на условията, регламентиращи употреба на кредитни или разплащателни карти.



4.2.17. Право на интелектуална собственост - включително авторски права.

Да се спазват правата на интелектуална собственост на доставчиците на съдържание. Материалите с авторско съдържание трябва да бъдат идентифицирани като такива. При използване на такива материали е необходимо да се получи писмено разрешение от носителя на авторските права за използване на авторско съдържание, включително търговски марки и лоба, текст, звук, фотографии, илюстрации и други файлове с изображения, аудио и видео.

4.2.18. Мрежови и локални дискове:

а) Мрежовите устройства на училището се използват за служебни цели. Служителите не трябва да съхраняват личен софтуер или файлове на никое мрежово устройство, собственост на училището.

б) Личната употреба на ИТ системи на училището, не е неприкосновена. Служителите нямат същите права на лична неприкосновеност, както в случаите, в които използват лични устройства, извън рамките на системи, собственост на училището. Служители, заподозрени в употреба на служебно оборудване за лични цели, носят отговорност за своите действия и могат да им бъдат поискани обяснения и предприети дисциплинарни наказания.

в) Ограниченията за мрежови устройства се прилагат и към локални дискове. Служителите не трябва да съхраняват на компютрите си забранени или неподходящи материали, софтуер или съдържание, което е обект на авторски права.

г) На потребителя се препоръчва да спазва следните правила:

1. Да създава име на работните документи (файлове) с латински букви, за да не възпрепятства възстановяването им при възникване на такава необходимост, включително и на файловете, които са съхранени с коректни имена на латиница.

2. Периодично да изпълнява процедура по запаметяване и архивиране на файловете, които обработва, за да предотврати загубата на данни от прекъсване на хранването или други непредвидени обстоятелства.

4.2.19. Съхранение на записи:

а) Служебни комуникации, които се изпращат по електронен път (например имейл съобщения) стават официални записи, и също са предмет на изискванията за съхранение на записи и официална документация.

б) Всякаква чувствителна информация на хартиен носител трябва да бъде отстранявана от бюрата и заключвана в шкаф в края на всеки работен ден и/или когато съответният служител ще отсъства.

Всички шкафове, съхраняващи чувствителна информация на хартиен носител, трябва да бъдат държани затворени и заключени в отсъствието на съответния отговорен за тях служител.

Ключовете за шкафове, съхраняващи чувствителна информация на хартиен носител, следва да не бъдат оставяни безнадзорно.

в) В края на всеки работен ден и/или при продължително отсъствие на съответния служител преносимите компютри трябва да бъдат осигурени срещу физически достъп от други лица като се прибират и заключват в шкафове или се заключват в кабинети с ограничен достъп.



г) Паролите за достъп до информационните системи на МОН или на училището, както и паролите за всички приложения, част от информационните системи на МОН или на училището, следва да не бъдат записвани на бележки или лепящи листчета.

д) Всички презентационни дъски в стаите за срещи и конференции следва да бъдат изтривани след завършване на съответната среща.

е) Всички външни носители на информация, собственост на училището, (CD/DVD/Blu-ray, USB флаш/хард дискове, карти памет и т.н.) трябва да бъдат третираны като устройства, потенциално съдържащи чувствителна информация, поради което следва да бъдат надлежно заключвани на места с ограничен достъп.

ж) Разпечатките от всички принтери, факсове и/или мултифункционални устройства в края на работния ден трябва да бъдат отстранявани и в случай, че техният собственик не може да бъде установен, следва да бъдат унищожавани в специализирано устройство тип „шредер“.

4.2.20. Достъп:

а) Достъпът до системи на МОН или училището може да се разрешава само от оторизирани служители, поради което останалите служители не трябва да се опитва да достъпва данни или програми, за които няма разрешение или изрично съгласие.

б) Ако служителите имат въпроси, свързани с достъпа до информационни системи, те трябва да се свържат с определеното от директора лице и съвместно да обсъдят въпроса.

4.2.21. При използване на лично устройство.

Вследствие на съображенията за наличие на рискове, свързани с личните устройства, служителите, които желаят да използват такива, трябва да получат формално разрешение и изрично да приемат изискванията на настоящата политика. Училището приема тази възможност само като опция и продължава да осигурява възможността за извършване на служебните задължения върху изцяло предоставен от него хардуер и софтуер за нуждите на служебната дейност.

Служителите трябва да спазват добрите практики и да не навлизат в личното пространство на околните (като например да извършват аудио-визуални записи на работното място с цел zlepоставяне или придобиване на служебна информация от друг служител).

4.2.22. Указания към мобилните устройства:

а) Мобилните средства да се използват само по предназначение и според нуждите на деловата дейност в училище.

б) Мобилните средства трябва да се съхраняват надеждно и да не се оставят без надзор. Ако това се налага, да се вземат мерки за физическа защита, например съхранение в охранявани помещения на доверени лица, сейфове на хотели или обществени трезори. Да не се предоставят на други лица за ползване без контрол.

в) Всеки отговорник на актив (мобилно средство) трябва да полага грижи за запазване целостта и пригодността за употреба на актива.

г) Всяко лице, ползващо мобилно средство, трябва да е запознато с правилата за неговата употреба.



4.2.23. Безжичен достъп в рамките на работните помещения:

а) Ако някой служител с мобилно устройство или гост на училището желае да използва достъп само до Интернет, то той може да го направи свободно, след предоставяне на активната парола. Мрежата, която предоставя достъп до Интернет на гости, не следва да има достъп до ресурси във вътрешноведомствената мрежа.

б) Безжичният достъп до информационните системи на училището следва да бъде контролиран и подсигурен съобразно добрите практики, а именно:

○ Безжичен достъп за общо ползване, предназначен за връзка към Интернет, следва да бъде логически, а където това е възможно, и физически отделен от вътрешната мрежа на училището;

○ Безжичният достъп за общо ползване следва да бъде подсигурен със силна парола (минимум 12 символа с необходимата комплексност, съгласно изискванията на настоящата политика), подлежаща на регулярна смяна за срок не по-дълъг от 6 месеца и да използва метод на автентификация поне WPAv2-Enterprise.

г) Безжичният достъп до информационните системи на училището, както и този, предоставящ Интернет свързаност, следва да се тестват регулярно срещу пробиви и уязвимости. След всеки тест, официален доклад от теста следва да бъде представен на директора.

4.2.24. Архивиране и възстановяване на файлове.

Всеки служител прави резервни копия на работните документи, които да му послужат при срив на системата.

4.2.25. Предаване, регистрация, отчетност и съхраняване на приетите документи в учреденския архив:

Съгласно Вътрешни правила за дейността на учреденския архив в ОУ „Христо Ботев“ – гр. Варна

4.2.26. Ред за достъп и ползване на архива на ОУ „Христо Ботев“ – гр. Варна:

Достъп до архивохранилището има само длъжностното лице, отговарящо за съхранението и използването на документите от архива, а в негово отсъствие – лица оторизирани да извършват контрол по опазването и съхраняването на документите.

4.2.27. Унищожаване на информационни активи на хартиен носител.

Поради невъзможността на хартиените носители да бъдат използвани повторно, всички непотребни информационни активи на такъв носител, трябва да бъдат унищожавани. Унищожаването следва да бъде правено в специализирано устройство от тип shredder.

4.2.28. Изваждане от употреба и унищожаване на ИТ оборудване:

а) Когато даден ИТ актив достигне края на полезния си живот в училище, той трябва да бъде предоставен на определено лице за подготовка за брак. В най-общия случай, това следва да се направи от съответното лице, което е функционален собственик на дадения ИТ актив, посредством подаване на заявка към ръководството;

б) Отговорното лице за изваждането от употреба и унищожаването на ИТ активи трябва по сигурен начин (посредством специализиран софтуер) да изтрие всички носители



на информация според добрите практики съгласно международно утвърдени стандарти за сигурно изтриване на данни, при извършване на минимум 2 цикъла, както следва:

1. всички данни, включително файлове и лицензиран софтуер трябва да бъдат изтрети със специализиран софтуер включен в списъка с допустим софтуер на училището;

2. за мрежови устройства – стартиращите и текущите конфигурации следва да бъдат изтрети, а където това е приложимо, следва да бъдат върнати заводските настройки на всяко едно устройство.

в) Сигурно изтритото и проверено ИТ оборудване да бъде свалено от отчет от списъка с ИТ активите на училището;

г) Сигурно изтритото и проверено ИТ оборудване да бъде маркирано със стикер, показващ, че информацията от съответното оборудване е сигурно изтрита;

д) Физическото отстраняване на ИТ оборудването може да стане чрез фирма за разделно събиране на отпадъци.

е) При никакви обстоятелства ИТ оборудване, подлежащо на брак, не трябва да бъде изхвърляно в неспециализирани контейнери, контейнери за общи отпадъци или подобни.

ж) При изваждане от употреба на ИТ оборудване, съдържащо полезна за училището информация, тази информация следва да бъде надлежно архивирана за срок не по-малък от 1 година и/или преместена на ново ИТ оборудване, преди унищожаването ѝ от оборудването, подлежащо на брак.

з) CD/DVD/Blu-ray дискове следва да бъдат физически унищожавани в устройство тип shredder или чрез счупване.

4.2.29. Връщане на активи.

Всички служители и потребители от трета страна при прекратяване на тяхното трудово отношение, договор или споразумение трябва да върнат всички ползвани от тях активи на училището, съгласно утвърдените вътрешни процедури.

4.3. Управление на сигурността на човешките ресурси. Подбор на кадри. Срокове и условия за наемане на работа.

4.3.1. Управление на сигурността на човешките ресурси:

а) Задължение на всеки служител е да се запознае с принципите за информационна сигурност, след което да попълни декларация, че е запознат и приема да спазва утвърдените правила за мрежова и информационна сигурност на ОУ „Христо Ботев“ – гр. Варна, както и да ги спазва при изпълнение на ежедневните си задължения.

б) Новопостъпилите служители да се информират за отговорностите си за спазване на вътрешните, правни и регулаторни изисквания за информационна сигурност чрез провеждането на първоначален инструктаж по отношение на информационната сигурност от определеното длъжностно лице и попълнят декларация, че са запознати и приемат да спазват утвърдените правила за мрежова и информационна сигурност на ОУ „Христо Ботев“ – гр. Варна.

в) Умишленото или неволно нарушаване на общоприетите принципи за информационна сигурност, подлежи на дисциплинарни санкции.

г) Всички служители и външни доставчици на услуги следва да получат необходимата за целите на тяхната дейност най-актуална информация относно изискванията за сигурност, мерките за контрол и уязвимостите, касаещи информационните системи на училището.



д) С цел намаляване на риска от умишлено или неумишлено предизвикани инциденти да се извършват регулярни обучения и инструктажи на служителите, имащи отношение към процесите и дейностите. Обученията и инструктажите да се провеждат за повишаване на знанията и компетенциите по отношение на мрежовата и информационна сигурност, както и за да се гарантира подходящата квалификация, знания и умения за изпълнение на отговорностите на служителите. Да се извършват не по-малко от два пъти годишно, като могат да бъдат и под формата на презентации, споделени обучителни материали, тестове, съобщения по електронната поща във връзка с конкретни заплахи и събития и др. Обученията и инструктажите да се извършват по предварително утвърден график и се организират, документират и контролират от определено лице.

Процесът при назначаване/напускане на служител, разпределение на задължения е подробно разписан в Приложение А от настоящите правила.

4.3.2. Подбор на кадри:

а) Назначаването на служители се извършва по „Основни процедури и работни инструкции описващи процесите при управление на човешките ресурси в ОУ „Христо Ботев“ – гр. Варна“, Приложение №1 Работна инструкция „Набиране и подбор на персонала“.

б) Срокове и условия за извършване на работа.

Всеки юридически субект, чиито служители работят или пребивават на територията на ОУ „Христо Ботев“ – гр. Варна по силата на договорни отношения, е длъжен да спазва изискванията на училището по отношение на ИС. За целта да се подпише двустранно споразумение за конфиденциалност (или Допълнение към договора), с цел доказване, познаване и приемане на тези изисквания и познаване последствията от тяхното неспазване. На база на тези документи е възможно евентуално последващо търсене на отговорност и съдебно производство.

в) Обучение.

Процедура за обучение на персонала се извършва по „Основни процедури и работни инструкции описващи процесите при управление на човешките ресурси в ОУ „Христо Ботев“ – гр. Варна“, Приложение №9 Работна инструкция „Планиране и организиране на обучението на персонала“.

г) Клауза за конфиденциалност.

Външни доставчици и консултанти, чиито дейности са пряко или непряко свързани с технологичната среда на училището, следва да подпишат клауза за конфиденциалност за всяка възложена им дейност. Само след като бъде подписано споразумението за конфиденциалност да се предостави на външните потребители необходимия достъп до ИТ инфраструктура, непублична информация и чувствителни данни на училището.

4.4. Сигурност на инфраструктурата.

Компонентите, изграждащи информационните системи, да съдържат интегрирани в тях функционалности, необходими за предоставянето на защитени и надеждни оперативни услуги. Работата с информационните системи да бъде съобразена с изискванията за информационна сигурност на училището, както и с правните и регулаторни изисквания.



Структурните компоненти, свързани със сигурността, да бъдат разработени, внедрени, конфигурирани и поддържани по начин, който не излага на уязвимости информационните системи. Последствията от евентуални оперативни рискове следва да бъдат намалени до приемливия минимум.

а) Контрол на логическия достъп:

За предотвратяване на рискове, свързани с нерегламентиран достъп до чувствителна информация, да се осъществява контрол на логическия достъп до тази информация.

Потребителските профили за достъп да се предоставят индивидуално и използват само от упълномощените служители, зачитайки предоставените им потребителски профил/роля/права за достъп за дадено приложение в съответната технологична среда на училището.

Индивидуално предоставения потребителски профил трябва да:

- бъде управляван чрез процедури за регистрация и прекратяване на права за достъп на потребител, приложими за информационни системи, за които съществува неоспоримо съответствие между потребителски идентификационен номер (ID) и служител. За всеки потребител на дадена система следва да има неоспоримо съответствие между потребителски идентификатор и служител, който единствен е упълномощен да го използва;
 - спазва принципа за минимум привилегировани права за достъп на служител до определена система, необходими, за да изпълнява ежедневните си служебни задължения;
 - съответства на предефинираните изисквания за разпределение на задълженията в училището;
 - бъде наблюдаван редовно, за да се предотвратят опити за неоторизиран достъп, и да се потвърди ефективността и ефикасността на процеса за контрол на логическия достъп;
 - съобразява автоматизирано или ръчно, описаните по-долу изисквания за комплексност на парола. Правилата за създаване на парола трябва да съответстват на последните заплахи и уязвимости, на които е подложена технологичната среда на училището.
- Комплексност на паролите:
 - Системни пароли:
 - Дължина: поне 15 символа;
 - Да съдържат поне две големи и две малки букви;
 - Да съдържат поне две цифри от 0 до 9;
 - Да съдържат поне два специални символа (например: ,!\$%^&*()_+|~- =\{}[]:~';<>?./).
 - Пароли за административен достъп до сървъри или инфраструктурни системи:
 - Дължина: поне 15 символа;
 - Да съдържат поне една голяма и една малка буква;
 - Да съдържат поне една цифра от 0 до 9;
 - Да съдържат поне един специален символ (например: ,!\$%^&*()_+|~- =\{}[]:~';<>?./).
 - Пароли за потребителски достъп, включително пароли за работни станции:
 - Дължина: поне 12 символа;
 - Да съдържат поне една голяма и една малка буква;
 - Да съдържат поне една цифра от 0 до 9;



- Да съдържат поне един специален символ (например: ,!\$%^&*()_+|~-=\{}[]:;'<>?,./).
- Използваемост на паролите:
 - Потребителите и администраторите не трябва да използват една и съща парола за достъп до различни системи и/или системни ресурси, освен в случай на липса на техническа възможност. Изключение правят ресурсите, които се достъпват със „single-sign-on“ през активната директория на МОН. (например: паролата за достъп до електронната поща следва да бъде различна от тази за достъп до счетоводната система или друга използвана система);
 - Всички потребители и/или администратори не трябва да използват пароли за достъп до системи на училището за свои лични нужди (например: паролата за достъп до електронната поща на училището следва да бъде различна от тази за достъп до личния адрес на електронната си поща).
- Смяна на паролите:
 - Всички системни пароли, които не се контролират от активната директория и служат за достъп до специфични ресурси, да бъдат ръчно променени поне веднъж на всеки шест месеца;
 - Всички потребителски и/или административни пароли, контролирани от активната директория, следва да бъдат променени посредством домейн политика поне веднъж на шест месеца;
 - Забранява се повторното използване на вече променена парола. За системните пароли, които не се контролират от активната директория, във всяка система следва да се настрои правило за следене, в случай че е възможно. За паролите, контролирани от активната директория, следва да се създаде домейн политика, която да ограничава преизползването на пароли;
 - При предоставяне на пароли на граждани във връзка с предоставени от училището услуги се допуска смяната на паролата за достъп да зависи от волята на потребителя.
- Защита на паролите:
 - Паролите да са строго персонални и по никакъв повод и при какво обстоятелство не следва да бъдат споделяни с трети лица, което се отнася както за служителите на работа, така и тези в отпуска. Паролите се считат за строго конфиденциална информация.
 - Паролите трябва да са персонифицирани. Изключение да правят системите, които не са свързани с активната директория и поради тяхното естество или спиране от поддръжка от страна на техния разработчик не позволяват достъп от повече от един потребител и/или администратор. В такъв случай е позволено използването на една парола от два или повече потребители и/или администратори, като този достъп трябва да бъде изрично одобрен от представител на ръководството.
 - При никакви обстоятелства паролите не трябва да бъдат изпращани по електронна поща, да бъдат записвани на хартиен носител, комуникирани по телефон, факс или друг несигурен или лесен за разчитане формат или канал.
 - Изключение може да бъде направено за новосъздадена парола, която задължително следва да подлежи на смяна при първо използване. Потребителското име, асоциирано със съответната парола, следва да бъде изпратено в различно съобщение.



- При никакви обстоятелства паролите не трябва да бъдат въвеждани в електронни анкети;
- При системи, предоставящи възможност за подсещане за паролата, подсещането не следва да включва части от паролата или нещо, което лесно би се асоциирало с паролата (например формата на паролата);
- Паролите не трябва да бъдат записвани във файл на работна станция, сървър или мобилно устройство в некриптиран вид. Единственото място, където паролите могат да бъдат записвани, е специализиран софтуер за мениджмънт на пароли;
- Възможността за „запаметяване на паролата“ в софтуерни приложения или уеб браузери следва да бъде ограничена – административно, посредством настоящата политика, и където това е възможно, технически – посредством домейн политика;
- Всеки потребител и/или администратор, който подозира, че неговата парола е компрометирана, следва да докладва този инцидент на определеното лице и да смени всички свои пароли за достъп до ресурси на МОН и училището.

Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издания им КЕП на трети лица, респективно да споделят своя PIN с трети лица.

По-високо ниво на достъп или достъп до система, до която лицето не трябва да има достъп в съответствие с възложените му служебни задължения, се предоставя при извънредни обстоятелства, когато е необходимо извършване на незабавни действия за защита на обществен интерес и те не могат да бъдат реализирани без получаване на достъп – извършва се по разпореждане на директора. Достъпът да се осигурява само за времето на изпълнение на задачата, след което се документират по подходящ начин възникналите обстоятелства, времето и основанието за достъпа.

Правата за достъп на служители, които временно или перманентно прекратяват служебните или трудово-правните си взаимоотношения с училището, се преустановяват.

б) Защита при обмен на информация.

Защитата при обмен на информация да бъде съобразена с нивото на класификация на управляваните данни в зависимост от използваните ресурси за комуникация. Критичните информационни ресурси да бъдат осигурени чрез прилагането на съвкупност от механизми за сигурност, следвайки принципа за “непробиваема защита”. Технологичната среда за обмен на данни да бъде поддържана и управлявана в зависимост от критичността на данните, системите и процесите, действащи в инфраструктурата от компютърни мрежи на училището.

в) Свързаност с вътрешни и външни комуникационни среди.

Една система може да бъде свързана към вътрешната мрежа на училището само след извършването на детайлен анализ на рисковете и след получено одобрение, при следните условия:

- да бъде управлявана в съответствие с изискванията за сигурност на информационните системи;
- да се поддържа от определен служител в училището или съответен доставчик на ИТ услуги;



- където е възможно директният достъп до критичните системи да бъде подсигурен с мултифакторна автентификация.

г) Мерки за сигурност при разработването на софтуер.

Доколкото разработването на софтуер е процес, който не се извършва от служители на училището, всички доставчици следва да бъдат задължени да спазват добрите индустриални практики при разработка на софтуер с оглед запазването на целостта, наличността и конфиденциалността на данните. За всеки нов програмен продукт следва да бъде извършван анализ на рисковете на база конфиденциалност на данните, които се обработват с помощта на приложението.

д) Управление на измененията в информационните системи и активи.

Извършваните промени не трябва да са в противоречие с принципите за информационна сигурност, като за целта трябва се осигури:

- извършване на тестове и ИТ одит проверки преди прилагане в експлоатация;
- предотвратяване на прекъсвания и/или спиране на дадена услуга;
- възможност за проследяемост и документиране на реализираните събития.

4.5. Физическа сигурност.

Ресурсите, използвани за развитие, управление и съхранение на чувствителна информация, да бъдат разположени в защитени помещения, осигурени чрез надеждни механизми за ограничаване на физическия достъп. Нивото на установената физическа сигурност трябва да бъде реализирано чрез подходящ баланс между *RFID* карти за идентифициране и технологии за наблюдение, които предотвратяват нерегламентиран достъп, влизане с взлом, заплахи, повреди или друг вид аварии и бедствия.

а) Сигурност на околната среда.

Да се предприемат специални превантивни мерки за разположението на компютърната техника и друг вид хардуер, осигуряващи сигурност срещу заплахи, предпоставка за които е околната среда - природни бедствия, повишена температура или влажност на околната среда.

Абсолютно забранено е изнасянето на техническо оборудване, собственост на училището, извън помещенията без да бъдат спазвани стриктно вътрешните процедури. Изключение са случаите, когато има изрично писмено разрешение на директора

Регламентирано за служебни цели е използването на мобилните устройства и преносими носители на информация, които са собственост на училището или са управлявани, съобразно принципите за сигурност. Хардуерът, софтуерът и обработваните данни, които са собственост на училището и се използват извън помещенията му, да са обект на същите процедури и механизми за сигурност, както прилаганите в училището.

г) Вътрешен контрол и одит:

Да се извършва периодичен контрол за съответствие с установените правила за сигурност на хардуера и софтуера на училището от определеното лице/лица от директора Той да обхваща необходимия минимум от дейности: цялостната конфигурация, преглед на минали събития, проверка на потребителски профили и контрол на нови версии (разлики при нови версии, създадени от доставчиците на софтуер).



Проверките, свързани със сигурността, да се провеждат поне веднъж годишно с цел контрол на: констатирани нередности и асоциираните с тях рискове, както и противодействащи мерки, които да ограничат вероятните рискове. Изпълнението на контролните дейности не трябва да са предпоставка за рискове, свързани със сигурността на информационните ресурси (примерно нарушаване на работния процес по време на одит, заплаха от нерегламентирани тестове.)

д) Управление на взаимодействията с трети страни.

При установяване на взаимоотношения с доставчици на стоки и услуги, наречени "трети страни", да се договорят изисквания за мрежова и информационна сигурност, включително:

1. за сигурност на информацията, свързана с достъпа на представители на трети страни до информация и активи на училището;
2. последици при неспазване на изискванията за сигурност на информацията;
3. 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;
4. 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.

В училището е определен служител/служители, отговарящ/отговарящи за спазване на изискванията по договорените изисквания за мрежова и информационна сигурност с „трети страни“ и параметрите на нивото на обслужване

5. Ангажираност на ръководството.

Директорът на училището, отговаря за разработването, внедряването, поддържането, развитието и подобряването на ефективността на системата за управление на информационната сигурност. Той лично насочва и създава единство на целите и ориентацията на училището като:

- Осигурява информирането на персонала на училището за важноста;
- Определя, актуализира и провежда правилата по сигурността;
- Провежда прегледи на СУИС (прегледи на сигурността);
- Осигурява ресурси за развитието и усъвършенстването на СУИС.

6. Съответствие, контрол и преглед.

Процедурите за контрол, свързани с прилагането на принципите, описани в текущите правила, са включени в процеса за постоянен контрол и задължителни за всички в училището. Контролът върху ефективността и ефикасността на процедурите е дейност делегирана на определени със заповед служители. Докладите с резултати от постоянния контрол да се предоставят на директора.



Приложение А - Процес при назначаване/напускане на служител, разпределение на задължения

Действие	Описание	Отговорник
1. Назначаване на нов служител.	Подготовка на трудов договор. Подписване на трудов договор. Инструктаж на служителя.	ЗАС Директор ЗДАСД
2. Справка за необходимите права за достъп, необходимата компютърна и комуникационна техника, и специализирания софтуер, с който ще работи служителя.	Права за достъп, компютърна и комуникационна техника, специализиран софтуер в зависимост от длъжностната характеристика.	ЗДАСД РНИКТ
3. Определяне на необходимостта от закупуване на нова техника или софтуер. Осигуряване на необходимата връзка към локалната мрежа.	При липса на съответстваща техника или софтуер се закупуват нови.	ЗДАСД РНИКТ
4. При предоставяне на вече ползван компютър се премахват всички данни от предишния потребител съобразно утвърдените в правилата за мрежова и информационна сигурност процедури.	Всички върнати за съхранение работни компютри са подготвени за нов ползвател съобразно утвърдените правила за мрежова и информационна сигурност.	РНИКТ
5. Запознаване с правилата на ползване на компютърната и комуникационната техника в ОУ „Христо Ботев“ – гр. Варна.	Всеки новопостъпил служител се запознава с вътрешните правилници и процедури на училището.	ЗДАСД РНИКТ
6. Извършва се кратко обучение и проверка дали новоназначения служител се е запознал с Вътрешните правила за мрежова и информационна сигурност.	Всеки новопостъпил служител преминава инструктаж на работното място.	ЗДАСД РНИКТ
7. Предоставяне на пароли за достъп до компютърната техника, служебната електронна поща и до информационните масиви, съпътстващи служебните задължения на служителя.	Паролите за достъп се предоставят в съответствие с длъжностната характеристика.	ЗДАСД РНИКТ
8. Проверка за необходимост от издаването на КЕП. Издаване на КЕП	КЕП се предоставя в съответствие с длъжностната характеристика на служителя.	ЗДАСД РНИКТ
9. Текущ контрол по време на работа на служителя за спазване на вътрешните правила за мрежова и информационна сигурност.	Текущият контрол е включен в План за контролна дейност на ЗДАСД.	ЗДАСД РНИКТ



10. Напускане на служител.	Заповед за прекратява не трудовото правоотношение.	Директор ЗАС
11. Временно/постоянно блокиране на достъпа до работното място при отсъствие/ напускане на служител.	При напускане се изтриват профилите и паролите на служителя.	РНИКТ
12. При напускане, служителя връща предоставените му от ОУ „Христо Ботев“ – гр. Варна технически средства, носители, КЕП и др.	Обходен лист.	Ресорен ЗД, домакин, библиотекар

Приложение Б - Функции на служителят, отговарящ за мрежовата и информационната сигурност

1. Борис Георгиев – РНИКТ ръководи дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност.
2. Проучва и анализира проблеми в информационната инфраструктура и предлага решения;
3. Участва и ръководи процеса по изготвяне на правилата и документираната информация свързана с мрежовата и информационна сигурност.
4. Следи за спазването на настоящите правила и прилагането на законите, подзаконовите нормативни актове, стандартите, политиките и правилата за мрежовата и информационната сигурност.
5. Консултира ръководството на училището във връзка с информационната сигурност.
6. Ръководи периодичните оценки на рисковете за мрежовата и информационната сигурност.
7. Периодично (не по-малко от веднъж в годината) изготвя доклад за състоянието на мрежовата и информационната сигурност в административното звено и го представя на директора.
8. Координира и предлага включване на служители в обученията, свързани с мрежовата и информационната сигурност.



9. Поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност.
10. Води регистър на инцидентите, свързани с мрежовата и информационна сигурност.
11. Уведомява РУО – Варна, за инцидентите, които имат въздействие върху непрекъснатостта на дейността на училището, най-малко 2 пъти:
 1. първоначално уведомяване, което се прави до два часа след констатирането на инцидента;
 2. в срок до 5 работни дни, като се предоставя пълната информация за инцидента.За целите на докладването следва да се използва Приложение № Г. на следната електронна поща: mariela.yankova@ruo.mon.bg.
12. Организира и участва в анализ на инцидентите с мрежовата и информационната сигурност за откриване на причините за тях и предприемане на мерки за отстраняването им с цел намаляване на еднотипните инциденти и намаляване на загубите от тях.
13. Следи за актуализиране на използвания софтуер и фърмуер.
14. Следи за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлага адекватни мерки за противодействието им.
15. Организира тестове за откриване на уязвимости в информационните и комуникационните системи и предлага мерки за отстраняването им.

Приложение В - Декларация на служителя

ДЕКЛАРАЦИЯ

за запознаване и спазване на **Правила за мрежова и информационна сигурност и допустимо използване на активи на ОУ „Христо Ботев“ – гр. Варна**

Аз, (трите имена)
потвърждавам, че съм прочел(а) и разбрал(а) Правилата за мрежова и информационна сигурност на ОУ „Христо Ботев“ – гр. Варна

Съгласен(на) съм да спазвам изискванията за достъп и употреба на ресурси.

Тази декларация е валидна за периода на моите трудови правоотношения с ОУ „Христо Ботев“ – гр. Варна, или до актуализирането на правилата.

Подпис: _____

Основно училище
гр. Варна, район Аспарухово
ул. „Кирил и Методий“ №8



„Христо Ботев“
тел. 052/370 696; 0877/446 812
e-mail: info-400026@edu.mon.bg

Длъжност: _____

Дата: _____

Приложение Г - Уведомление за инцидент свързан с информационната сигурност

Информация	Детайли
<i>До 2 часа от установяване на инцидента</i>	
Лице, подаващо уведомлението	Име, фамилия
Телефонен номер	
Електронна поща	
Училище	
Лице за контакт	Име, телефонен номер и поща на лице, което при необходимост да подаде допълнителна информация
Дата и час	Дата и час на възникване на инцидента, ако не е възможно – дата и час на откриване
Тип на инцидента	(Virus, Malware, Trojan.....)
Кратко описание на инцидента, като се описва и кои услуги са засегнати	
Източник на атаката (ако е налична информация)	IP address, DNS и т.н.
Предприети действия	