ЧЕТВЪРТО ОСНОВНО УЧИЛИЩЕ “ХРИСТО БОТЕВ”
гр. Лом - 3600, обл. Монтана, ул. “Софийска” 56, тел.: 0971/66548,
e-mail: ou_hbotev_lom@abv.bg

ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ
във IV Основно училище „Христо Ботев“ град Лом

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата Политика за мрежова и информационна сигурност е приета, съгласно изискванията на ЗЕУ, Закона за киберсигурност и чл. 4, ал.1 от Наредбата за минималните изисквания за мрежова и информационна сигурност и е одобрена със

Заповед № №РД-13-138/15.04.2021 година

Чл. 2. Настоящата политика за мрежова и информационна сигурност определя ред, отговорности, способи и средства при осъществяване контрол и управление на работата на информационните системи във IV Основно училище „Христо Ботев“ - град Лом, както и дейностите, които трябва да се предприемат, за отговор на всякакъв вид инциденти, свързани със сигурността на информационните активи и отрицателно въздействие върху поверителността, целостта и наличността на информацията. В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми.

Чл. 3. Документът касае и е приложим в работата на всички служители в институцията. Потребителите на информационни системи във IV Основно училище „Христо Ботев“ - град Лом са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 4. Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

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

РАЗДЕЛ II
КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

Чл.6. (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, IV Основно училище „Христо Ботев“ 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 рамките на IV Основно училище „Христо Ботев“ или извън него без никакво отрицателно въздействие върху училището, някой от неговите партньори, и/или свързани лица.	(а)Финансови отчети, публикувани до обществени 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 IV Основно училище „Христо Ботев“, 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 IV Основно училище „Христо Ботев“, 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. 7. 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. 8. 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. 9. 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. 10. 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. 11. 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. 12. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 13. 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. 14. На служителите във IV Основно училище „Христо Ботев“ - град Лом, 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. 15. 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. 16. При изнасяне на носители извън физическите граници на IV Основно училище „Христо Ботев“ - град Лом, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 17. 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. 18. 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. 19. 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. 20. Събирането, подготовката и въвеждането на данни на интернет страницата се извършва от оправомощени служители на IV Основно училище „Христо Ботев“ - град Лом. Длъжностните лица притежават потребителски имена и пароли за актуализиране на сайта.
Чл. 21. 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 общината.

РАЗДЕЛ IV
РАБОТНО МЯСТО

Чл. 22. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.
Чл. 23. 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. 24. 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. 25. 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. 26. 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. 27. Забранява се на външни лица работата с персоналните компютри на IV Основно училище „Христо Ботев“ - град Лом, 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. 28. След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off.
Чл. 29. 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. 30. 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. 31. Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства се извършва само след съгласуване със Системния администратор.
Чл. 32. 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 IV Основно училище „Христо Ботев“ - град Лом.
Чл. 33. 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. 34. 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. 35. Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до Системния администратор.
Чл. 36. 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. 37. 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 IV Основно училище „Христо Ботев“ - град Лом.
Чл. 38. Ползването на компютърната мрежа и електронна поща от служителите става чрез получените потребителско име и парола.
Чл. 39. Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и

необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.
Чл. 40. Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронна поща при използване на предоставените им потребителски имена и пароли.
Чл. 41. Компютрите, свързани в мрежата на общината използват интернет само от доставчици, с които IV Основно училище „Христо Ботев“ - град Лом има сключен договор за доставка на интернет.
Чл. 42. Забранява се свързването на компютри едновременно в мрежата на IV Основно училище „Христо Ботев“ - град Лом и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на IV Основно училище „Христо Ботев“ - град Лом 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. 43. Забранява се инсталирането и използването на комуникатори (като icq, skype, социални мрежи и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на IV Основно училище „Христо Ботев“ - град Лом 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 IV Основно училище „Христо Ботев“ - град Лом.
Чл. 44. Забранява се съхраняването на сървърите на IV Основно училище „Христо Ботев“ - град Лом на лични файлове с текст, изображения, видео и аудио.
Чл. 45. 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. 46. 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. 47. 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 срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация. При възстановяване на мрежата, всички локално запазени файлове следва да се преместят отново на сървъра и да се изтрият локалните копия.

РАЗДЕЛ VIII
СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 48. Осигурява се автоматизирано създаване на резервни копия на всички бази данни и електронни документи.

Чл. 49. 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 IV Основно училище „Христо Ботев“ - град Лом, утвърдени със Заповед на Директора на училището.

РАЗДЕЛ IX
УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Чл. 50. 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. 51. 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. Ръководителите и служителите във IV Основно училище „Христо Ботев“ - град Лом са длъжни да познават и спазват разпоредбите на тази 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 IV Основно училище „Христо Ботев“ - град Лом може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

Изготвил: **/п/ (**чл. 4, т.1 във вр. с чл.5, т.1, в)
от Регламент (ЕС) 2016/679)
Дафинка Борисова

Приложение №1

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ
към секторния ЕРИКС

Необходима информация	**Детайли**	**Данни**
(до 2 часа)		
Лице, подаващо уведомлението	Име, фамилия	
Вашият телефонен номер	(GSM)	
Вашата електронна поща		
Организация	Наименование на организацията, засегната от инцидента	
Лице за контакт (за целите на разрешаването на инцидента)	Име, телефонен номер и електронна поща на компетентно лице от предприятието, което при необходимост може да подаде допълнителна информация.	
Дата и час	Вписват се датата и часът на възникване на инцидента, ако не е възможно - датата и часът на откриването му.	
Тип на инцидента		0 Virus 0 Trojan 0 Botnet 0 Dos/DDos 0 Malware 0 Port Scan 0 Spam 0 Phishing 0 Pharming 0 Probe 0 Crack 0 Copyright 0 Ransomware 0 Defacement 0 Exploiting known Vulnerabilities 0 Application Compromise 0 Login Attempts 0 SQL injections 0 Unknown 0 Other

Кратко описание на инцидента	Вписва се кратко описание на инцидента, като се включва всяка практическа/техническа информация (тази информация се предоставя, в случай че е налична).	
Трансгранично въздействие	• Вписва се информация за евентуално трансгранично въздействие и се посочват държавите • Вписва се информация за услугите, които са засегнати	
Въздействие върху други съществени услуги	Вписва се информация на кои други съществени услуги евентуално ще окаже въздействие	
Засегната система (попълва се, ако е налична информацията)	IP Address: DNS: Operating System	
Източник на атаката (попълва се, ако е налична информацията)	IP Address: DNS:	
Предприети действия	Описват се първоначалните действия, предприети до момента - до 2 часа от засичането на инцидента.	
Публично оповестяване	Съгласно комуникационна стратегия на администрацията.	
до 5 работни дни		
Механизъм на атаката	Описва се механизмът на атаката	
Предприети действия	Описват се подробно действията, предприети за разрешаване на инцидента.	
Необходимост от коригиращи действия	Има ли необходимост от промяна в настройките на защитните стени, WAF или др. Промяна на политиката за сигурност, ако се налага Обучение на персонала	

Анализ на артефакти	Описват се резултатите от анализа на артефактите, ако има установени такива, и инструментите, използвани за това. Изпраща се копие от артефактите	
Публично оповестяване	Съгласно комуникационна стратегия на администрацията	

Забележка. Попълва се допълнителна информация в случай на необходимост.