ОСНОВНО УЧИЛИЩЕ „РАН БОСИЛЕК”

5300 Габрово, ул. “Орлово гнездо” №12, тел.: 066 / 807 516

e-mail: info-700102@edu.mon.bg

УТВЪРЖДАВАМ:

НИНА МИТЕВА

Директор на ОУ „Ран Босилек“ - Габрово

Политика за мрежова и информационна сигурност в ОУ„Ран Босилек“ за учебната 2024/2025 година

РАЗДЕЛ I.
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата Политика за мрежова и информационна сигурност се утвърждава на основание чл. 1, ал. 1, т. 1 от Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС № 186 от 26.07.2019 г.,) и имат за цел осигуряването на контрол и управление на работата на информационните системи в ОУ „Ран Босилек“ - Габрово. 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. 2. Потребителите на информационни системи в ОУ„Ран Босилек“ - Габрово са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3. Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Наредбата за минималните изисквания за мрежова и информационна сигурност.

РАЗДЕЛ II.
КОНТРОЛ НА ДОСТЪП И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 4. 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 на достъп до информация.

Регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация.

Техниката да се използва изключително и само за служебни цели.

Не се позволява инсталирането на какъвто и да е нов и реконфигурирането от потребителите на вече инсталиран софтуер и хардуер, както и самостоятелни опити за поправка или подобрения на горепосочените.

Не се позволява използването на внесени отвън софтуер и хардуер.

Използването на внесени отвън информационни носители (оптични дискове, флаш памети и др.) става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, носителите не се използват.

Не се допускат външни лица до комуникационните шкафове и техниката за интернет - връзка, с изключение на техници от оторизирани фирми и то само придружени от ръководителя на направление ИКТ или заместник-директор АСД..

Не се допуска достъпа на външни лица до компютърната техника в канцеларииите в сградата на ОУ „Ран Босилек“ - Габрово.

Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.

Паролите за достъп на всички служители, описани по видове приложения се съхраняват от ръководителя на направление ИКТ. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 5. Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизират, така че да може да бъде идентифициран. Не е разрешено използването на групови профили.

Чл. 6. Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретно информационни ресурси, според заемната длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

Чл.7. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн.

Чл. 8. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 9. Всички носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп.

Чл. 10. На служителите на ОУ„Ран Босилек“ - Габрово, които използват електронни бази данни и техни производни се забранява:

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

Чл. 11. 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.

Чл. 12. При изнасяне на носители извън физическите граници на ОУ„Ран Босилек“ - Габрово, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 13. На служителите е строго забранено да използват служебни мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него.

Чл. 14. 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 с шредер. Предварително се проверят, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

РАЗДЕЛ III.
РАБОТНО МЯСТО

Чл. 15. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 16. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място.

Чл. 17. Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява чрез потребителско име и парола.

Чл. 18. Забранява се на външни лица да работят с персоналните компютри на ОУ „Ран Босилек“, освен за:

- упълномощени фирмени специалисти в случаите на първоначална инсталация на компютърна и периферна техника, програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствие на директор, заместник-директор АСД или ръководителя на направление ИКТ;
- провеждане на обучения на външни педагогически специалисти по програми и проекти на МОН или РУО, но само след разрешението на Директора на училището и задължително в присъствието на ръководителя на направление ИКТ.

Чл. 19. След края на работния ден всеки служител задължително изключва компютъра, на който работи.

Чл. 20. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява ръководителя на направление ИКТ, който му оказва съответна техническа помощ.

Чл. 21. 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. 22. 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 с ръководителя на направление ИКТ.

Чл. 23. 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 ОУ „Ран Босилек“.

Чл. 24. 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. 25. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача.

Чл. 26. Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи - идентификация на потребител, пароли, отчитане на времето на достъп, забрани за копиране, проследяване на несанкциониран достъп.

Чл. 27. 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.

РАЗДЕЛ IV.
ПОЛЗВАПЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 28. Компютрите, свързани в мрежата на ОУ „Ран Босилек“, използват интернет само от доставчик, с когото училището има сключен договор за доставка на интернет.

Чл. 29. Фирмата, доставчик на интернет услугата:

- изгражда вътрешна мрежа с необходимите мрежови комутатори, рутери, защитни стени;
- избира техническите устройства, извършва необходимите настройки за достъп до интернет;
- разделя логически локалната мрежа на отделни мрежи - локална мрежа за администрация, локална мрежа за учители, локална мрежа за ученици и създава потребителски имена и пароли за работа с компютърната мрежа.

Чл. 30. Ползването на компютърната мрежа и електронните платформи /Admin+, Уча се, Електронни учебници и др./ от служителите става чрез получените потребителско име и парола.

Чл. 31. 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. 32. 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 електронните платформи при използване на предоставените им потребителски имена и пароли.

Чл. 33. Забранява се свързването на компютри едновременно в мрежата на ОУ „Ран Босилек“ и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на училището и/или е в противоречие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл.34. Използването на комуникатори (skype, facebook, messenger, viber, zoom и др.), осигуряващи достъп извън рамките на компютърната мрежа на ОУ „Ран Босилек“ 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 училището, да е ограничено и единствено и само за служебна цел.

Чл. 35. Забранява се съхраняването на компютрите на ОУ „Ран Босилек“ на лични файлове с текст, изображения, видео и аудио.

Чл. 36. Забранява се отварянето без контрол от страна на системния администратор на:

- 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;

➢ получени по електронна поща съобщения, които съдържат неразбираеми знаци.

Чл. 37. Не се толерира влизането в Интернет - сайтове с неизвестно съдържание.

РАЗДЕЛ V.
ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 38. С цел антивирусна защита се прилагат следните мерки:

➢ Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява.

Ръководителят на направление ИКТ извършва следните дейности:

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

➢ настройва антивирусния софтуер за периодични сканирания през определен период;

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

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

При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира ръководителя на направление ИКТ.

РАЗДЕЛ VI.
НЕПРЕКЪСПАТОСТ НА РАБОТАТА

Чл. 39. Следните мерки се прилагат с цел антивирусна защита:

➢ При липса на ел. захранване за повече от 10 мин., ръководителя на направление ИКТ започва процедура по поетапно спиране на устройствата за съхранение на данни;

➢ При срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация.

РАЗДЕЛ VII.
СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 40. Всеки служител, който работи с класифицирана информация, осигурява автоматично създаване на архивни копия всекидневно.

Чл. 41. Информацията, включително тази, съдържаща лични данни, се резервира по следните начини:

➢ Автоматизирано и планово се извършва архивиране на цялата работна информация на запаметяващите устройства и дисковите масиви.

➢ Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг компютър и да се продължи работният процес без чувствителна загуба на данни.

РАЗДЕЛ VIII.
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в ОУ „Ран Босилек“ са длъжни да познават и спазват разпоредбите на тази Политика.

§ 2. Контролът по спазване на Политиката се осъществява от ръководството на ОУ „Ран Босилек“.

§ 3. Настоящата политика се разглежда и оценява периодично с оглед ефективността им, като ОУ „Ран Босилек“ може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Тази Политика е разработени съгласно Наредбата за минималните изисквания за мрежова сигурност и влизат в сила от датата на утвърждаването и със Заповед на Директора на ОУ „Ран Босилек“.