123 СУ " Стефан Стамболов" – р-н " Красна поляна " – София
ул. „ Братин дол" 26, Тел: 920 30 23,
mail: sou123@abv.bg

ПОЛИТИКА ЗА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ

РАЗДЕЛ I. ОСНОВНИ ПОЛОЖЕНИЯ

Чл. 1. С настоящата политика се уреждат управлението, контрола и използването на информацията, публикувана в интернет пространството, информацията в мрежовата система и използването на компютърното оборудване в 123 СУ „Стефан Стамболов".

Целта на тази политика е:

- да гарантира ефикасното и безопасно използване на компютърната техника ;
- да гарантира, че служителите ще използват предоставените им компютри и интернет връзка в съответствие с изпълнението на служебните им задължения и само за тази цел;
- да предотврати възможно застрашаване целостта на информацията в мрежовата инфраструктура на 123 СУ „Стефан Стамболов".

Чл. 2. Всички компютри са свързани чрез мрежа и не се толерира никакво застрашаване на тази система.

Чл. 3. Правилата важат за всички служители, работещи в 123 СУ „Стефан Стамболов" със служебни компютри.

РАЗДЕЛ.РАЗПРЕДЕЛЕНИЕ НА РОЛИТЕ И ОТГОВОРНОСТИ

Чл. 4. Директорът на 123 СУ „Стефан Стамболов"

Директорът на 123 СУ „Стефан Стамболов" се ангажира със системата за управление на мрежовата и информационна сигурност като:

- носи пряка отговорност за мрежовата и информационната сигурност на училището, включително и за дейности, които се възлагат на трети страни;
- създава условия за прилагане на комплексна система от мерки за управлението на мрежовата и информационната сигурност по смисъла на междунаро-

ден стандарт ISO/IEC 27001:2013;
- осигурява наличието на ресурсите, необходими за СУМИС;
- упражнява контрол чрез организиране на одити и годишни прегледи на мрежовата и информационна сигурност;

определя със заповед служител(и), отговарящ(и) за мрежовата и информационната сигурност в 123 СУ „Стефан Стамболов“;
- насърчава подобряването на СУМИС

Чл.5. Служител по мрежова и информационна сигурност

Служителят по мрежова и информационна сигурност (СМИС) се назначава на основание чл. 3, ал. 2 от НМИМИС.

Със заповед за „Служител по мрежова и информационна сигурност“ (СМИС) е назначена Десислава Илиева

СМИС осъществява функции, свързани с организирането, управлението и прилагането на мерки за мрежова и информационна сигурност

РАЗДЕЛ III. ДОСТЪП И ПАРОЛИ

Чл. 6. Достъпът до Интернет, електронната поща и компютърното оборудване, осигурени от и предоставени на 123 СУ „Стефан Стамболов“ са само за служебно ползване. Използването им за лични цели е забранено.

Чл. 7. Забранява се достъпа до компютърните файлове на други служители. Разрешение за това дава съответния потребител, при наличието на основателна причина - отсъствие на служител.

Чл. 8. Паролите за достъп до служебните компютри и програмни продукти, се съхраняват от самите служители.

Чл. 9. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.

Чл. 10. Всеки служител има лична парола и персонална идентификация, която не предоставя за използване от други лица и е достатъчно защитена.

Чл. 11. При съмнение за нарушение на сигурността на личните данни, лицето, което е установило несъответствието (случайно или неправомерно унищожаване на лични данни, загуба, промяна, неразрешено разкриване или нерегламентиран достъп), незабавно уведомява служителят по мрежова и информационна сигурност.

РАЗДЕЛ IV. РАБОТА С ПРОГРАМНИ ПРОДУКТИ

Чл. 12. 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.

Чл. 13. При съмнение за възникнал проблем при работа с програмен продукт, незабавно се уведомява служител по мрежова и информационна сигурност, екипът на Админ Софт и/или съответните оторизирани фирми, разработили програмния продукт.

Чл. 14. Използването на внесени отвън информационни носители (оптични дискове, дискети, флаш памети и др.) става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, носителите не се използват.

Чл. 15. Инсталирането на софтуерни програми, нямащи отношение към пряката служебна работа е ЗАБРАНЕНО!

РАЗДЕЛ V . ИЗПОЛЗВАНЕ НА ИНТЕРНЕТ И ЕЛЕКТРОННА ПОЩА

Чл. 16. Достъпът до Интернет става чрез инсталирани на персоналните компютри браузър.

Чл. 17. Не се разрешава използването на Интернет връзката за гледане на видео или филми от служителите, което значително намалява скоростта на връзката на другите служители.

Чл. 18. Правилата за достъп на служителите до Интернет включват следните задължителни изисквания:

1. Не се толерира влизането в Интернет - сайтове с неизвестно съдържание;
2. Използването на чат - програми е единствено и само за служебна цел;
3. Не се разрешава тегленето на файлове с неизвестно съдържание от Интернет;
4. Ползването (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, файловете се изтриват незабавно.

Чл. 19. Достъпът до електронна поща на 123 СУ „Стефан Стамболов“- sou@abv.bg се осъществява от директора и заместник-директори учебна дейност.

Съобщения, изпратени от ел. поща на училището са законосъобразни и подлежат на изпълнение.

Всички съобщения се изпращат, в изпълнение на отговорности, подписани, с имена и длъжност.

При отсъствие на директора, в заповедта за заместване се конкретизира длъжностно лице, на което е даден достъп до ел. поща на 123 СУ „Стефан Стамболов“.

Чл. 20. Правилата за достъп и използването на електронната поща, включват следните задължителни изисквания:

1. Служителите не трябва да отварят съобщения, получени от неизвестен получател или неизвестна Интернет страница. Такива съобщения се изтриват незабавно.
2. Прикачените файлове към съобщенията, получени в служебните пощи, не се отварят при съмнение за вируси.

Чл. 21. Служителите преместват важната информация от получените съобщения в отделни файлове върху техните компютри.

РАЗДЕЛ IV. РАБОТА С КОПИР, ПРИНТЕР, СКЕНЕР

Чл. 22. (1) Не се допуска:

1. Самостоятелни опити за поправка на принтерна, копирна и друга техника. При съмнение за съществуващ проблем служителите следва да се обръщат към оторизирана фирма.
2. Смяната на тонер-касети и отстраняването на заседнали листи се извършва на място, само от обучени за това служители.
3. Техниката се използва изключително и само за служебни цели;

РАЗДЕЛ VI . АРХИВИРАНЕ И УНИЩОЖАВАНЕ (ИЗТРИВАНЕ) НА ЕЛЕКТРОННИ ДОКУМЕНТИ

Чл. 23. Създадените файлове от служителите на персоналните им компютри, както запазените файлове от съобщенията в електронните пощи, които вече не са необходими с оглед изпълняването на служебните задължения, се изтриват периодично.

Чл. 24. С цел недопускане на загуба на информация, всяка важна информация се съхранява в диск "D " на компютъра, както и на преносима памет, която периодично се

актуализира.

РАЗДЕЛ VII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 25. Настоящата политика е разработена в съответствие с чл. 4 от Наредбата за минималните изисквания за мрежова и информационна сигурност, заповед № СОА20-РД09-5095/23.12.2020 г. на Кмета на СО и е утвърдена със заповед на директора на 123 СУ „Стефан Стамболов“.

Подлежи на актуализиране при промяна на нормативната база.

Чл. 26. За нуждите на настоящата политика е извършен вътрешен одит за мрежова и информационна сигурност в организацията , създадени са работни бланки , блокови схеми и др. необходими документи за правилното и прилагане .