



6000 Стара Загора, ул. "Сава Силов" 69, п.к. 195, тел. 042/641004 директор,
тел 042/631003 зам.-директор, тел. 042/629189 канцелария, e-mail:soumgstz@abv.bg
Web site:www.soumgstz.info

ПОЛИТИКА ЗА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ В СУ „МАКСИМ ГОРКИ“

РАЗДЕЛ I. ОСНОВНИ ПОЛОЖЕНИЯ

Чл.1. С настоящата политика се уреждат управлението, контрола и използването на информацията, публикувана в интернет пространството (сайт и фейсбук страница на училището), информацията в мрежовата система и използването на компютърното оборудване в СУ „Максим Горки“.

(1) Целта на тези правила е:

1. да гарантира ефикасното използване на персоналните компютри;
2. да гарантира, че служителите ще използват предоставените им служебни компютри и Интернет връзка в съответствие с изпълнението на служебните им задължения и само за тази цел;
3. да предотврати възможно застрашаване целостта на информацията в мрежовата инфраструктура на СУ „Максим Горки“.

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 СУ „Максим Горки“ със служебни компютри.

РАЗДЕЛ II. ДОСТЪП И ПАРОЛИ

Чл.4. Достъпът до Интернет, електронната поща и компютърното оборудване, осигурени от и предоставени на СУ „Максим Горки“ са само за служебно ползване. Използването им за лични цели е забранено.

Чл.5. Забранява се достъпът до компютърните файлове на други служители. Разрешение за това дава съответният потребител, при наличието на основателна причина.

Чл.6. Паролите за достъп до служебните компютри и програмни продукти, се съхраняват от самите служители.

Утвърдена със заповед № РД – 553/14.09.2020г.

Чл.7. Служителите не могат да предоставят паролите си за достъп до системата на други служители, външни лица, роднини и приятели.

Чл.8. (1) Всеки служител има лична парола и персонална идентификация, която не предоставя за използване от други лица и е достатъчно защитена.

Чл.9. 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 директора.

РАЗДЕЛ III. РАБОТА С ПРОГРАМНИ ПРОДУКТИ

Чл.10. 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.11. При съмнение за възникнал проблем при работа с програмен продукт, незабавно се уведомява оторизираното за тази цел лице от звеното по киберсигурност, експертът по Информационно осигуряване в РУО-Стара Загора, екипът на АдминСофт, съответните оторизирани фирми , разработили програмния продукт

Чл.12. Използването на внесени отвън информационни носители (оптични дискове, дискети, флаш памет и др,) става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, носителите не се използват.

Чл.13. Инсталирането на софтуерни програми, несъотнесими към пряката служебна работа е ЗАБРАНЕНО.

РАЗДЕЛ III. ИЗПОЛЗВАНЕ НА ИНТЕРНЕТ И ЕЛЕКТРОННА ПОЩА

Чл.14. Достъпът до Интернет става чрез различни браузъри.

Чл.15. Не се разрешава на учители и служители използването на Интернет връзката за гледане на видео или филми несвързани с учебната работа.

Чл.16. 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 инсталирането на други чат-програми, освен Skype;
4. Не се разрешава тегленето на файлове с неизвестно съдържание от Интернет;
5. 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.17. Достъпът до електронна поща на СУ „Максим Горки“ soumgstz@abv.bg се осъществява от директора, заместник-директори, а гл. счетоводител, ЗАС и касиер – домакин имат лични служебни електронни пощи.

1. Постъпилата информация по ел. поща, касаеща дейността на гл. счетоводител, ЗАС (писма, справки НАП, извлечения и информация за банкови преводи, искания за справки и др.) се препраща към техните лични служебни пощи.
2. Съобщения, изпратени от ел. поща soumgstz@abv.bg на СУ „Максим Горки“ са законосъобразни и подлежат на изпълнение.
3. Всяко съобщение, което ЗДУД, главен счетоводител, ЗАС изпращат в изпълнение на отговорности от техните служебни ел. адреси, трябва да е обозначено и видимо, че е от тях.

Чл.18. 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.19. Служителите преместват важната информация от получените съобщения в отделни файлове в техните компютри.

РАЗДЕЛ IV. РАБОТА С КОПИР, ПРИНТЕР, СКЕНЕР

Чл.20. (1) Не се допуска 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 V. АРХИВИРАНЕ И УНИЩОЖАВАНЕ (ИЗТРИВАНЕ) НА ЕЛЕКТРОННИ ДОКУМЕНТИ

Чл.21. 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.22. С цел недопускане на загуба на информация, всяка важна информация се съхранява в диск различен от този, на който е инсталирана ОС на компютъра.

РАЗДЕЛ VI. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл.23. Настоящата политика е разработена в съответствие с Постановление № 186 от 19 юли 2019 г. за приемане на Наредба за минималните изисквания за мрежова и информационна сигурност и са утвърден със заповед № 553/14.09.2020г. на директора на СУ „Максим Горки“. Подлежи на актуализиране при промяна на нормативната база.

Чл.24. Настоящата политика се преразглежда редовно, но не по-рядко от веднъж годишно, и при необходимост се актуализира.