32.СРЕДНО УЧИЛИЩЕ С ИЗУЧАВАНЕ НА ЧУЖДИ ЕЗИЦИ
„СВЕТИ КЛИМЕНТ ОХРИДСКИ“

гр. София, бул. „Христо Ботев“ №63, тел.: 02/9874358,
email: kl_ohridski32@school32.com

УТВЪРЖДАВАМ:

Д-Р НЕЛИ КИРКОВА-КОСТОВА,

ДИРЕКТОР НА 32. СУИЧЕ

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В 32. СРЕДНО УЧИЛИЩЕ С ИЗУЧАВАНЕ НА ЧУЖДИ ЕЗИЦИ „СВЕТИ КЛИМЕНТ ОХРИДСКИ“

РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите Вътрешни правила са разработени на основание чл. 1, ал. 1, т. 1, чл. 5, ал. 1, т. 6 , т. 7 и чл. 8, ал. 1 от Наредбата за минималните изисквания за мрежова и информационна сигурност и имат за цел осигуряването на контрол и управление на работата на информационните системи в 32.СУИЧЕ.

Чл. 2. Потребителите на информационни системи в 32.СУИЧЕ са длъжни със своите 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 разпоредбите на нормативната база.

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

Чл. 4. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

(1) разделяне на потребителски от администраторски функции;

(2) установяване на нива и достъп до информация;

(3) регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;

(4) осъществяването на контрол.

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 оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили.

Чл. 6. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез средствата на активна директория с конкретно

потребителско име, осигурено от Системния администратор/ оторизираното за това лице, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 7. Предоставянето на достъп става 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. 8. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн.

Чл. 9. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 10. Всички носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп.

Чл. 11. На служителите на 32.СУИЧЕ, които използват електронни бази данни и техни производни (текстове, разпечатки, имена, ЕГН и др.) 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 и разрешение от директора на училището;

Чл. 12 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. 13 При изнасяне на носители извън физическите граници на 32.СУИЧЕ, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 14 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. 15 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. 16 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. 17. Събирането и подготовката на данните се извършва от служителите, след което данните се изпращат в електронен вид (на файлове) на служителите, отговорни за качването им на интернет страницата 32.СУИЧЕ

Чл. 18. Въвеждането на данни на интернет страницата се извършва от служител/и на 32.СУИЧЕ, определен/и със заповед на Директора на училището.

РАЗДЕЛ III. РАБОТНО МЯСТО

Чл. 19. Всеки служител работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола.

Чл. 20. 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. 21. Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения, обособени за целта в сградата на 32.СУИЧЕ, съобразени с мерките за противопожарна защита.

Чл. 22. Работата на външни лица работата с персоналните компютри на 32.СУИЧЕ е забранена. Изключение се допуска 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, като дейностите се извършват задължително в присъствие на Системния администратор или на изрично определен служител от директора на 32.СУИЧЕ.

Чл. 23. След приключване на извършването на определена дейност на компютър всеки служител задължително излиза от профила си (привежда го в режим log off), а в края на работното си време излиза от профила си (log off) и изключва компютъра (shut down).

Чл. 24. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Системния администратор/оторизираното за това лице, който му оказва съответна техническа помощ.

Чл. 25. 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. 26. 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 от Системния администратор/оторизираното за това лице.

Чл. 27. Забранява се инсталиране на приложения които не са свързани с преките служебни задължения на служителя.

Чл. 28. Служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните си задължения.

Чл. 29. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача, при спазване на принципа „необходимост да се знае”.

Чл. 30. Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

РАЗДЕЛ IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 32. Системният администратор/оторизираното за това лице извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща в 32.СУИЧЕ.

Чл. 33. Ползването на компютърната мрежа, служебна електронна поща и други платформи от служителите става чрез получените потребителско име и парола.

Чл. 34. Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност за не спазване на задължението си.

Чл. 35. Компютрите, свързани в мрежата на 32.СУИЧЕ използват интернет само от доставчик, с когото училището има сключен договор за доставка на интернет.

Чл. 36. Забранява се свързването на компютри едновременно в мрежата на 32.СУИЧЕ 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 нормативната база.

Чл. 37. Забранява се инсталирането и използването на комуникатори (като facebook, viber, skype и др.), осигуряващи достъп извън рамките на компютърната мрежа на 32.СУИЧЕ и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер.

Чл. 38. Съхраняването на лични файлове с текст, изображения, видео и аудио-записи на сървърите на 32.СУИЧЕ е забранено.

Чл. 39. Забранява се отварянето на получени по електронна поща съобщения / файлове, които съдържат неразбираеми знаци.

РАЗДЕЛ V. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 40. С цел антивирусна защита се прилагат следните мерки:

(1) Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява.

(2) Системният администратор извършва следните дейности:

2.1. настройва антивирусния софтуер за периодични сканирания през определен период;

2.2. активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на системата;

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

(3) При поява на съобщение от антивирусната програма за вирус, всеки служител от съответното работно място задължително информира Системния администратор.

РАЗДЕЛ VI. СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 41. Системния администратор/оторизираното за това лице осигурява автоматизираното създаване на резервни копия на всички база данни и електронни документи.

РАЗДЕЛ VII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Всички служители в 32.СУИЧЕ са длъжни да познават и спазват разпоредбите на Вътрешните правила. Веднъж годишно преминават инструктаж за повишаване на вниманието им по отношение на мрежовата и информационна сигурност. Попълват декларация за спазване на политиката за мрежова и информационна сигурност - образец 1 към настоящите правила.

§ 2. Контролът по спазване на правилата се осъществява от Директора на училището или упълномощено със заповед лице (системен администратор).

§ 3. Настоящите Вътрешни правила подлежат на актуализация при промяна на нормативната база.

§ 4. Вътрешните правила за мрежова и информационна сигурност са утвърдени със заповед на директора на 32. СУИЧЕ „Св. Климент Охридски“ № ……../……...г. и влизат в сила от датата на утвърждаването им.