ДЕТСКА ГРАДИНА С ЯСЛЕНИ ГРУПИ № 95 „ОМАЙНИЧЕ”
Столична община, район „Люлин”; тел. 02/927-74-55; e-mail: dg95box@gmail.com

УТВЪРЖДАВАМ:
ДИРЕКТОР НА
ДЕТСКА ГРАДИНА № 95 „ОМАЙНИЧЕ“

ПЕТЯ ДИМОВА

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ДГ №95 „ОМАЙНИЧЕ“

Раздел I. ОБЩИ ПОЛОЖЕНИЯ.

Чл.1. Настоящите Вътрешни правила се утвърждават на основание чл. 1, ал. 1, т. 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 ДГ № 95 „Омайниче“ - гр. София.

Чл.2. (1) Целта на настоящите вътрешни правила е да гарантират, че служителите на детската градина ще използват предоставените им компютри и интернет връзка за изпълнение на служебните им задължения и едновременно с това да предотвратят възможността за застрашаване целостта на информацията в мрежовата инфраструктура на ДГ № 95 „Омайниче“.

(2) Вътрешните правила са задължителни за спазване от всички служители на ДГ № 95 „Омайниче“.

Чл.3. „Информационна система“ е съвкупност от компютърна и периферна техника, програмни продукти, данни на 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. Програмните продукти и бази данни могат да бъдат специфични за всеки служител или с общо предназначение.

Чл.4. Проектирането, изграждането и обновяването на информационни и комуникационни системи в ДГ № 95 „Омайниче“ се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда при спазване на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл.5. (1) Потребителите на информационни системи в ДГ № 95 „Омайниче“ са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

(2) Достъпът до интернет, електронната поща и компютърното оборудване, осигурени и предоставени от ДГ № 95 „Омайниче“ са само за служебно ползване.

Използването им за лични цели е забранено.

(3) Забранява се достъпа до компютърните файлове на други служители, освен в тяхно присъствие и с тяхното изрично разрешение и/или по компетентност.

Чл.6. За да се следи за изпълнението на настоящите вътрешни правила е възможно да се извършва мониторинг на компютрите, включително преглед на съдържанието на файловете в компютрите. Това става с разрешението на директор на ДГ.

Раздел II. КОНТРОЛ НА ДОСТЪПА

Чл.7. (1) Правилата за достъп на служителите до информационната система на ДГ гарантират по-добрата организация, по-висока сигурност и по-ефективната работа с компютърната техника, предоставена на служителите на ДГ № 95 „Омайниче“.

(2) Правилата за достъп на служителите включват следните задължителни изисквания:

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

2. На работното място 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. Инсталират се само програмни продукти обезпечаващи конкретната работата на служителя. При съмнение за възникнал проблем незабавно се уведомява директорът или упълномощено за това лице.

3. Използването на внесени 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.

4. Паролите за достъп до служебните компютри и програмни продукти, се съхраняват от самите служител.

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

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

7. Дължината на паролата трябва да е най-малко 8 знака, като знаците да са комбинация от числа, големи и малки букви и символи.

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.

9. Не се допускат външни лица до сървърното помещение, сървърните шкафове и техниката за интернет - връзка, с изключение на техници от оторизирани фирми, и то само придружени от служител на ДГ.

Чл.8. 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.

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

Чл.10. (1) Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заемната длъжност и функция.

(2) Не се задава и не се осигурява достъп на неоторизирани лица.

Раздел III. ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл.11. Всички носители на данни се съхраняват в безопасна и сигурна среда - в съответствие със спецификациите на производителите, в заключени шкафове, с ограничен и контролиран достъп.

Чл.12. На служителите на ДГ, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици и др.) се забранява:

1. Да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството.

2. Да ги използват извън рамките на служебните си задължения.

3. Да ги предоставят на външни лица без разрешение на директора на ДГ.

Чл.13. 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.14. При изнасяне на носители извън физическите граници на ДГ № 95 „Омайниче“, те се поставят в подходяща опаковка и в запечатан плик.

Чл.15. На служителите е строго забранено да използват служебни мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него. Потребителите на служебни мобилни компютърни средства и служебни мобилни телефони отговарят за защитата им от кражба и не ги оставят

без наблюдение.

Чл.16. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл.17. 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.18. При съмнение за възникнал проблем при работа с програмен продукт, незабавно се уведомява експерта по Информационно осигуряване в РУО - София, екипа на АдминСофт, ръководител на проект „Програмни продукти за детски заведения", съответните оторизирани фирми, разработили програмния продукт.

Раздел IV. ИЗПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА, ИНТЕРНЕТ И ЕЛЕКТРОННА ПОЩА

Чл.19. При наличие на сървър той се разполага в самостоятелни помещения, обособени за целта в сградата на ДГ, съобразени с мерките за противопожарна защита.

Чл.20. (1) Служителите имат право да работят на служебен компютър, като достъпът до съхраняваните данни се осъществява с въвеждането на потребителско име и парола.

(2) Забранява се на външни лица да работят с персоналните компютри на ДГ, 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 изрично определен служител от ДГ.

Чл.21. След края на работния ден всеки служител задължително изключва компютъра, на който работи.

Чл.22. (1) 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.

(2) При загуба на данни или информация от служебния компютър, служителят незабавно уведомява директора, системния администратор или оторизираното за това лице, който му оказва съответна техническа помощ.

Чл.23. 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, Viber и Messanger.

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.24. (1) Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица.

(2) За неизпълнение на задължението си по ал.1 виновните служители носят дисциплинарна отговорност, както и в случаите когато 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.25. Компютрите, свързани в мрежата на ДГ, използват интернет само от доставчик, с когото ДГ има сключен договор за доставка на интернет.

Чл.26. Забранява се свързването на компютри в други мрежи и/или друго, което е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и Наредбата за минималните изисквания за мрежова и информационна сигурност (в сила от 26.07.2019 г.).

Чл.27. Използването на електронната поща на ДГ е само за служебна цел. 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 се отварят при условие, че първо те се сканирани за наличието на вируси. Ако антивирусният софтуер намери такива, файловете се изтриват незабавно.

3. Старите съобщения, които вече не са необходими с оглед изпълняването на служебните задължения, трябва да бъдат периодично изтривани.

4. Служителите трябва да преместват важната информация от получените съобщения в отделни файлове върху техните компютри.

Чл.28. Достъпът до електронна поща на ДГ № 95 „Омайниче“ -

dg95box@gmail.com и info-2212777@edu.mon.bg се осъществява от директора, ЗАС, гл. счетоводител и касиер-домакина, които имат служебна електронна поща.

1. Постъпилата информация по ел. поща , касаеща дейността на счетоводител, ЗАС /писма, справки НАП, съобщение РМС - заплащане наем, фактури , извлечения, информация за банкови преводи, искания за справки и др./ се препраща към техните лични служебни имейли.

2. Съобщения, изпратени от ел. поща на ДГ – dg95box@gmail.com и info-2212777@edu.mon.bg са законосъобразни и подлежат на изпълнение.

3. Всяко съобщение, което директор, главен счетоводител и касиер-домакин изпращат в изпълнение на отговорности от техните служебни ел. адреси, е подписано от тях с имена и длъжност.

4. Получените служебни електронни писма се регистрират във входящия дневник на ДГ № 95 “Омайниче“.

5. При отсъствие на директора, в заповедта се конкретизира длъжностно лице, на което е даден достъп до ел. поща на ДГ № 95 „Омайниче“.

Раздел V. КОПИРНА, ПРИНТЕРНА И ДРУГА ТЕХНИКА

Чл.29. 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 оторизираната фирма „ЕВОТЕК“.

2. Изнасянето на вече направени разпечатки, съдържащи примерно технически грешки, лични данни или информация за ДГ. Същите трябва да бъдат унищожавани чрез накъсване със съответната техника.

3. Смяната на тонер-касети и отстраняването на заседнали листи да се извършва на място, само от обучени за това служители. За смяната се информира отговорното лице за осигуряване на консумативи.

Чл.30. Техниката се използва изключително и само за служебни цели;

Раздел VI. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.31. С цел антивирусна защита се прилагат следните мерки:

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

2. Антивирусният софтуер трябва да е настроен за периодични сканирания на файловите системи на компютрите за вируси.

3. Защитната стена на системите да е активна, освен в случаите когато работата с определени продукти или услуги на други институции не изискват различни настройки.

4. Софтуерът да е правилно настроен за автоматично обновяване на операционната система и инсталираните програмни продукти.

5. При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира директора, системния администратор или оторизираното за това лице.

6. 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. СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл.32. Счетоводните данни и данните от работата с други програмни продукти се архивират ежедневно. При наличие на споделените документи те се архивират ежеседмично.

Чл.33. 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.

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 VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Служителите в ДГ № 95 „Омайниче" са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от счетоводителя на ДГ № 95 „Омайниче" или лично от директора.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично – ежегодно с оглед ефективността им. Директорът на ДГ № 95 „Омайниче" може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Промени в настоящата инструкция се извършват със заповед на директорът на ДГ № 95 „Омайниче".

§ 5. Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност (в сила от 26.07.2019 г.).

§ 6. Вътрешните правила влизат в сила от датата на утвърждаването им със Заповед № 68/ 28.09.2026 г. на директора на ДГ № 95 „Омайниче".