ДЕТСКА ГРАДИНА № 57 “ХОСЕ МАРТИ”
София 1359, район “Люлин”, ул.“501”, №1
тел.:02 825 38 20/02 825 09 75; e-mail: cdg57@abv.bg

Утвърждавам!
Директор:
Емилия Караиванова

ВЪТРЕШНИ ПРАВИЛА
ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ДГ №57 „ХОСЕ МАРТИ“ гр.София

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 №57 „Хосе Марти“-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 динадетската гра.

(2) Вътрешните правила са задължителни за спазване от всички служители на ДГ.

Чл.3. „Информационна система“ е 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. 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 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 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 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.

(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. 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.

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

6. Паролите за достъп на всички служители, описани по видове приложения се съхраняват от директора на ДГ или от друго посочено от него лице .

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

8. Следните дейности са строго забранени: опити за неоторизиран достъп до компютърната система, повредата или разрушаването на компютърното оборудване, софтуер или информация.

Чл.8. 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 е от специализирани звена посочени от директора или лично.

Чл.9. 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.10. Всички пароли за достъп на системно ниво се променят периодично.

Чл.11. (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.12. 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.13. 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.14. 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.15. При изнасяне на носители извън физическите граници на ДГ, те се поставят в подходяща опаковка и в запечатан плик.

Чл.16. 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.17. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до злоумишлен софтуер. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл.18. 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.19. Събирането, подготовката и въвеждането на данни на страницата се извършва от служители на ДГ, определени със заповед на Директора.

Чл.20. Събирането и подготовката на данните се извършва от служители в техния ресор, след което данните се изпращат в електронен вид (на файлове) на служителите отговорни за качването им на

интернет страницата на ДГ.

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

Чл.21. При наличие на сървър той се разполага в самостоятелни помещения, обособени за целта в сградата на ДГ, съобразени с мерките за противопожарна защита.

Чл.22. (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.23. След края на работния ден всеки служител задължително изключва компютъра, на който работи.

Чл.24. (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.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 или оторизираното за това лице.

Чл.27. 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 ДГ. При неотложна необходимост се спазват правилата за антивирусна защита, като се вземат мерки за неразпространяване на информацията и нейното използване по предназначение в ДГ.

Чл.28. Служителите имат право да обменят компютърна информация само във връзка с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

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 компютърна информация, бази данни и софтуер се ограничава посредством технически методи или други правила- идентификация на потребител, пароли, отчитане на времето на достъп, забрани за копиране, проследяване на несанкциониран достъп.

Чл.31. Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

Чл.32. Системния администратор или 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 ДГ.

Чл.33. (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.34. Компютрите, свързани в мрежата на ДГ, използват интернет само от доставчик, с когото ДГ има сключен договор за доставка на интернет.

Чл.35. 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.36. (1) Забранява се инсталирането и използването на комуникатори (социални мрежи), като facebook, icq, skype и др. подобни, създаващи предпоставки за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на ДГ.

(2) Инсталирането на комуникатори (социални мрежи) става само след изричното разрешение на директора на ДГ.

Чл.37. Забранява се съхраняването на сървърите на ДГ на лични файлове.

Чл.38. Забранява се отварянето без контрол от страна на системния администратор или оторизираното за това лице на:

1. 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;

2. получени по електронна поща съобщения, които съдържат неразбираеми знаци;

3. използването на неподходящи, обидни или порнографски Интернет страници;

4. използването на Интернет връзката за гледане на видео или филми от служителите, което значително намаляват скоростта на връзката на другите служители.

Чл.39. Разрешава се използването на чат - програми е единствено и само за служебна цел.

Чл.40. 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.

5. Получените служебни електронни писма се регистрират във входящия дневник на ДГ.

Раздел V.
КОПИРНА, ПРИНТЕРНА И ДРУГА ТЕХНИКА

Чл.41. 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 определеното от директора лице за решаване на проблема.

2. Работата на външни лица с наличната копирна, принтерна и друга техника, както и техни опити за отстраняване на възникнали проблеми, освен на лица - служители на оторизираните за това фирми, със знанието директора или определено за това лице.

3. 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.

Чл.42. 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.43. Винаги се поддържа резервен („втори“) консуматив за копирната техника с оглед непрекъснатост на работата.

Раздел VI.
ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.44. 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. Да е активирана защитата на различните програмни продукти за предупреждение при наличие на зловреден софтуер. 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.

Раздел VII.
СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл.47. При наличие на системния администратор или оторизираното за това лице то осигурява автоматизираното създаване на резервни копия на всички база данни и електронни документи всеки ден. В противен случай служителите архивират важните данни на място определено от директора и различно от персоналното по график определен от него.

Чл.48. Счетоводните данни и данните от работата с други програмни продукти се архивират ежедневно. При наличие на споделените документи те се архивират ежеседмично.

Чл.49. 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.

Раздел VIII.
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Служителите в ДГ са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от счетоводителя на ДГ или лично от директора.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично – ежегодно с оглед ефективността им. Директорът на ДГ 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.

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

§ 6. Инструкцията влиза в сила от датата на утвърждаването ѝ със Заповед на директора на ДГ.