

РЕПУБЛИКА БЪЛГАРИЯ
АДМИНИСТРАТИВЕН СЪД - БЛАГОЕВГРАД



УТВЪРЖДАВАМ:

/Стоянка Пишиева - Сахатчиева/
Председател на
Административен съд - Благоевград
Дата: 28.04.2025г.



ВЪТРЕШНИ ПРАВИЛА
ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИЯТА, ИЗПОЛЗВАНЕ НА
КОМПЮТЪРНОТО ОБОРУДВАНЕ И ПЕРИФЕРНИ УСТРОЙСТВА, ИНТЕРНЕТ,
МРЕЖОВИ РЕСУРСИ И ОРГАНИЗАЦИЯ НА ДОСТЪПА ДО ТЯХ В
АДМИНИСТРАТИВЕН СЪД - БЛАГОЕВГРАД

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1 (1) Настоящите правила определят правата, задълженията и отговорностите на потребителите на единната компютърна и информационна система в Административен съд – Благоевград.

(2) Потребители са всички органи и служители на Административен съд – Благоевград, както и лицата, ползващи компютърните ресурси на съда на друго основание.

(3) Правилата са разписани за гарантиране ефикасното използване на компютрите; за гарантиране, че съдиите и служителите ще използват предоставените им компютри и Интернет връзка в съответствие с изпълнението на служебните им задължения и само за тази цел; за предотвратяване възможно застрашаване целостта на информацията.

Чл. 2. Правилата са част от разработката на стратегия за защита на служителите и съда. Всички компютри са свързани в защитена мрежа, която е недостъпна и не подлежи на застрашаване от външни фактори.

Чл. 3. (1) Правилата важат за всички съдии и съдебни служители, работещи в Административен съд – Благоевград.

(2) Правилата, относно използването на информацията и компютърното оборудване, следва да се спазват. Заобикалянето им под каквато и да е форма не е разрешено.

(3) Всеки потребител носи лична отговорност за действията си, независимо от действащите механизми за сигурност в тази насока.

Чл. 4. (1) Тези правила са разработени съгласно НАРЕДБА за минималните изисквания за мрежова и информационна сигурност, приета с ПМС № 186 от 19.07.2019 г., обн., ДВ, бр. 59 от 26.07.2019 г., в сила от 26.07.2019 г.

(2) Поради бързия напредък в областта на информационните технологии, този документ подлежи на периодичен преглед на съдържанието и актуализация на разписаните норми. Потребителите са задължени да спазват описаните правила.

II. ОСНОВНИ ПРАВИЛА НА ИНФОРМАЦИОННАТА ПОЛИТИКА

Чл. 5. Основните права и задължения за осигуряването и поддържането на компютърната и информационна среда в Административен съд – Благоевград са на системния администратор.

Чл. 6. (1) Всички работни станции се включват в единна локална мрежа на Административен съд – Благоевград. Изключение правят работните станции за работа с класифицирана информация.

(2) С цел защита на системния и приложния софтуер, компютърната мрежа и защита на работните документи на служителите, всички ползватели на локалната компютърна мрежа в съда имат само потребителски права върху персоналните си компютри и строго дефинираните им мрежови ресурси.

(3) Всички компютърни програмни продукти и информация, създадени и съхранени от потребителите, са собственост на съда.

(4) На компютрите се правят типови инсталации на програмни продукти в зависимост от изпълненията на служебните задължения на служителите и съобразно притежаваните към момента налични лицензи.

(5) Допълнителен софтуер може да бъде инсталиран само след утвърдена заявка във връзка с възникнала служебна необходимост, като се следи за чистота от

гледна точка на лицензите, авторските права и липса на конфликт с останалите приложения.

Чл. 7. Целта на тези вътрешни правила е да гарантира ефикасното използване на компютрите и останалата офис 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 на целостта на информацията.

Чл. 8. Потребителите се задължават да спазват правилна експлоатация на хардуерните, периферните устройства и софтуерните продукти, които ползват при оптимални разположение и настройки.

III. СПЕЦИФИЧНИ ФУНКЦИИ по поддържане и защита на информационните и компютърните системи

Чл. 9 Във връзка с чл. 5. от настоящите правила, Системният администратор:

(1) Подготвя и инсталира необходимите компютърни системи (хардуер) и софтуер;

1. Разполага компютърната техника по оптимален начин след съобразяване с техническите и материалните ресурси и възможности на работното помещение и работното място - разположението на видеомонитора, клавиатурата и работещия с тях трябва да отговаря на следните изисквания: разстояние между очи и екран 0,50-0,70м разстояние между очи и клавиатура 0,45-0,50м.;

2. За правилно охлаждане на устройствата, в близост и върху тях да не се поставят книги, хартия, дрехи, саксии с цветя и други вещи, като преносимите компютри да се поставят върху равна и права повърхност за оптимално охлаждане. Стационарно монтираните устройства не се преместват от определените им места;

3. Не се допуска попадане на чужди тела и течности в устройствата. В близост до устройствата и върху тях не трябва да се слагат съдове с напитки и хранителни продукти. Не се поставят устройства по первазите на прозорците и други рискови места;

4. В случай на продължително отсъствие на потребител (пет и повече работни дни) от работа (командировка, отпуска, болнични, обучение или др.), системният администратор изключва офис техниката, която ползва потребителя и от контактите. За продължително отсъствие по смисъла на изречение 1 служителят, назначен на длъжността „Човешки ресурси“ уведомява системния администратор;

(2) За всеки потребител създава „акаунт“ (валидно потребителско име и парола), осигуряващ му идентификация и достъп до персоналния компютър и мрежовата среда на Административен съд – Благоевград.

(3) Оказва методическа помощ на служителите при работата им с компютърните системи и софтуер.

(4) Извършва оценка и одобрение на използвания софтуер и хардуер, включително на подбора на доставчици на интернет и информационни услуги.

(5) Разработва, внедрява и поддържа системи за препятстване и контрол на нерегламентиран достъп до информация и бази данни.

(6) Внедрява и поддържа антивирусен софтуер.

(7) Разработва, внедрява и поддържа системи за авторизация и идентификация при влизане и излизане от компютърните системи.

(8) Реализира концепции за защита и опазване на електронните бази данни.

(9) Подменя части, добавя компоненти, принадлежности и други за подобряване на компютърните конфигурации, както и текуща подмяна на дефектирала техника. Гаранционното обслужване на техниката се извършва само от упълномощените за това фирмени сервиси.

(10) Внасянето и изнасянето на компютърна и периферна техника от административната сграда на Административен съд – Благоевград става само в присъствието на системния администратор.

(11) При прекратяване на служебното (трудовете) правоотношение между Административен съд – Благоевград и определен служител, Съдебният администратор уведомява системния администратор не по-късно от 3 работни дни преди датата на прекратяване. С изтичане на работния ден, предхождащ прекратяването на правоотношенията на служителя с Административен съд – Благоевград, системният администратор прекратява правата на достъп до мрежови ресурси, електронна поща и компютър на служител, чието служебно (трудовете) правоотношение с Административен съд – Благоевград се прекратява и при необходимост извършва преинсталация на компютъра. Потребителски акаунт на напуснал служител може да бъде активен до 30 календарни дни от датата на напускането с права само за четене на кореспонденцията в случаите, когато служителят е водел служебна кореспонденция с външни организации.

Чл. 10. За отстраняване на възникнали проблеми, диагностика и поддръжка на системите да се оказва съдействие на системния администратор, включително с осигуряване на физически и отдалечен достъп до компютъра с всички необходими пароли. Ако това са пароли на директория с ограничен достъп, те се обслужват само от технически лица, имащи съответния допуск за работа с такава информация.

IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИТЕ

Чл. 11. Всеки потребител има право на оборудвано с персонален компютър работно място и може да използва в своята работа софтуера, собственост на Административен съд – Благоевград.

Чл. 12. Всеки потребител има право на персонален служебен e-mail адрес и име към т.нар. „служебна електронна поща" (*****@bl-adc.justice.bg) на Административен съд – Благоевград, те се съхраняват на мейл сървър - @bl-adc.justice.bg, който е защитен с мейл протектор, предотвратяващ спам, спайуеър и т.н. зловреден код. Персоналният електронен адрес в структурата на Административен съд - Благоевград се образува от първата буква от името на потребителя и фамилията му, разделени с точка и изписани на латиница.

Чл. 13. (1) Всеки потребител има право на достъп до служебна информационна страница на Административен съд – Благоевград, както и достъп до деловодната система на съда с правомощия, според спецификата на длъжността. Всеки потребител разполага с персонална идентификация и лична парола.

(2) За приложения, които изискват обслужване с пароли, паролите трябва да бъдат с годност 90 дни;

(3) За приложения, за които не е нужно обслужване и годност на паролите, изискванията са следните:

1. Дължина на паролата - минимум 8 /осем/ символа, от които един да бъде цифра, и поне една главна буква;

2. Заклучване на паролата след 3 последователни неуспешни опита за правилно изписване.

Чл. 14. За всякакви възникнали въпроси във връзка с използването на компютърната техника и информационните системи потребителят следва да се обръща към системния администратор.

Чл. 15. Всички потребители имат право на достъп до интернет при изпълнение на присъщите им служебни задължения или за други цели в интерес на Административен съд – Благоевград.

Чл. 16. Достъпът до Интернет, електронната поща и компютърното оборудване, осигурени от Административен съд – Благоевград са само за служебно ползване. Използването им за лични цели е забранено.

Чл. 17. Потребителите нямат право да копират или унищожават файлове с данни, които са създадени във връзка с тяхната работа.

Чл. 18. Потребителят е задължен да се грижи за опазването на данните, които са необходими за неговата дейност, да спазва правилата, които осигуряват

цялост, валидност и конфиденциалност на използваните данни, по начин по който при възникване на програмен или технически проблем максимално бързо да се възстановят щетите и да се възобнови нормалния процес по изпълнение на служебните задължения.

Чл. 19. Забранява се достъпът до компютърните файлове на други служители, освен личните. Разрешение за това дава съответният потребител, при наличието на основателна причина. За да се следи изпълнението на тази политика, може да бъде извършван мониторинг на компютрите. С цел осъществяване на техническата поддръжка, с разрешението на ръководството на съда, при необходимост се извършва преглед на съдържанието на файловете в компютрите.

Чл. 20. Ръководството има право да контролира ползването на програмните продукти, електронната поща, интернет и базите данни.

Чл. 21. Достъп до официалната електронна поща на съда имат Председателят на съда, съдебният администратор и системният администратор.

Чл. 22. Логическият достъп на потребителите е подробно описан в създадените групови и индивидуални акаунти на сървъра – домейн контролер. Той се определя от системния администратор на всеки съд, при съгласуваност с ръководителя на организационната единица, в зависимост от това с кои звена в организацията комуникира даденият потребител и какви мрежови приложения ползва.

Чл. 23. Във връзка с информационните технологии и ползването на компютърните и информационните системи, на потребителите не се позволява:

(1) 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. При съмнение за възникнал проблем, незабавно се уведомява системният администратор.

(2) Използването на внесени отвън информационни носители, както и внесени отвън софтуер и хардуер.

(3) Копиране на лицензираните компютърни програми с цел лична употреба или предоставянето им на други лица или организации.

(4) Разлепването и унищожаването на гаранционните лепенки, както и инвентарните такива, поставени върху компютърните кутии.

(5) Допускането на външни лица до сървърното помещение, комуникационните шкафове, и техниката за интернет – връзка, с изключение на техници от оторизирани фирми и то само придружени от системния администратор.

(6) Злонамерена увреда или умишлено разрушаване на компютърното оборудване, софтуер или информация.

(7) Отстъпването на паролите си за достъп до системата на други служители и/или трети лица.

(8) Ползването на лични пароли и персонална идентификация.

(9) Използването на чуждо потребителско име и парола.

(10) Извършването на дейност, която застрашава целостта на компютърната мрежа или атакува други системи.

(11) Заобикаляне на системите за сигурност, намаляване на сигурността на локалната мрежа или бази данни.

(12) Ползването на активно съдържание, като Active X контроли и Java аплети, които позволяват по време на използването на Интернет в системата на потребителя да проникнат вируси или друг зловреден софтуер.

(13) Ползването на неподходящи Интернет страници и такива със съмнително съдържание, както и тегленето на файлове с неизвестно съдържание от Интернет.

(14) Извършването на модификация на файл, който не е създаден от тях, освен при наличието на основателни причини или при съгласието на създалия файла потребител.

(15) Нерегламентиран достъп до данни, за които потребителят няма права.

(16) Използване на служебната електронна поща за нужди извън служебната кореспонденция.

(17) Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност.

(18) Използването на мрежата за извършване на стопанска или незаконна дейност.

(19) Ползването на ресурсите за развиване или подпомагане на чужд бизнес.

Чл. 24. Използването на FTP следва да е само за администраторски цели, през предварително зададен нестандартен порт. Достъп да имат само потребители със създадени акаунти и пароли на интернет – сървър.

Чл. 25. При обмен на файлове в локалната мрежа се използват точно определените за конкретната дейност споделени папки с регламентирани права за достъп.

V. СИГУРНОСТ И СЪХРАНЕНИЕ НА ИНФОРМАЦИЯТА В АДМИНИСТРАТИВЕН СЪД – БЛАГОЕВГРАД

Чл. 30. Информацията, съхранявана на сървъра на Административен съд – Благоевград е защитена посредством персонална парола за достъп на системния

администратор. Част от информацията на сървъра е достъпна за всички потребители в мрежата на Административен съд – Благоевград чрез достъп до Public (HP-SERVER) - регламентирано пространство на сървъра, достъпно за споделяне на файлове и документи от всички потребители в мрежата.

Чл. 31. Въведени са конкретни мерки за защита на информационните и компютърните системи срещу компютърни вируси, срыв на локалните мрежи, прекъсване на електрозахранването и др., както следва:

(1) Използване на лицензирана антивирусна програма ESET ANTIVIRUS

(2) Всички сървъри и устройства за съхранение на данни да са свързани към устройство за непрекъсваемост на ел. снабдяването /UPS/.

(3) Нов потребител:

1. Всички заповеди за създаване на нови потребители трябва да бъдат подписани от Председателя на съда;

2. Заявките трябва да бъдат съхранявани от системния администратор за срок не по-малък от една година;

3. За всеки потребител се създава „акаунт“ (валидно потребителско име и парола), осигуряващ му идентификация и достъп до съответната част от ресурсите, след изрична заповед.

Чл. 32. (1) Архивирането на информацията се извършва ежедневно на външен носител, съхраняван от системния администратор.

(2) 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.

(3) Базите данни на всички програми се архивират по предписанията, направени от производителя.

(4) Резервните копия се съхраняват на носител, различен от този, на който са разположени данните или електронните документи.

(5) Споделените документи се архивират 2 пъти седмично.

(6) Съхраняват се най - малко последните 7 резервни копия.

Чл. 33. При срыв в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация. При възстановяване на мрежата, всички локално запазени файлове, следва да се преместят отново на сървъра и да се изтрият локалните копия.

VI. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 34. Служителите на Административен съд – Благоевград познават и спазват разпоредбите на тези правила, за което се задължават с подписването на декларация по Образец, приложение към този документ.

Чл. 35. Контролът по спазване на правилата се осъществява от съдебния администратор и системния администратор.

Чл. 36. При неспазване на задълженията и правилата за работа с компютърната система, посочени в тези вътрешни правила, потребителите носят дисциплинарна и имуществена отговорност в съответствие с действащото законодателство.

Чл. 37. Настоящите Вътрешни правила са утвърдени със Заповед №РД-13-46/28.04.2025г. и влизат в сила от 28.04.2025г.

Настоящите Вътрешни правила влизат в сила от датата на тяхното утвърждаване.

Правилата да се публикуват на интернет страницата на Административен съд – Благоевград и да се разпространят чрез локалната мрежа на съда.

ИЗГОТВИЛ СИСТЕМЕН АДМИНИСТРАТОР:
/инж. Людмил Мездрички/



ПРИЛОЖЕНИЕ А – ФОРМУЛЯР ЗА СЪГЛАСИЕ С ПОЛИТИКАТА

Декларирам, че съм прочел/а и разбирам Вътрешните правила, описани в настоящия документ:

.....

Съгласен/а съм да спазвам изискванията на настоящите Вътрешни правила, както и последващи промени, за които ще бъда директно информиран/а по електронен или друг път.

Съгласен/а съм дейността ми в Административен съд – Благоевград да бъде наблюдавана в рамките, очертани в настоящите Вътрешни правила.

Съзнавам, че всяко нарушение на Вътрешните правила може да доведе до дисциплинарни санкции.

Име:.....

Подпис:

Дата.....