РЕПУБЛИКА БЪЛГАРИЯ
АДМИНИСТРАТИВЕН СЪД - МОНТАНА

ПОЛИТИКА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Уредбата в областта на мрежовата и информационна сигурност е регламентирана в Закона за киберсигурност, обн. - ДВ, бр. 94 от 13.11.2018 г. и Наредба за минималните изисквания за мрежова и информационна сигурност, приета с ПМС № 186 от 19.07.2019 г., Правилника за вътрешния ред за използването на електронен подпис и електронна идентификация от органите на съдебната власт.

1. Общи положения

1.1. Настоящата политика определя общите изисквания по отношение механизмите за контрол върху информационните технологии с цел осигуряване на по-висока сигурност и гарантиране пълнотата, своевременността и валидността на данните и опазване целостта им.

1.2. Политиката е насочена към:

- намаляване риска от неоторизиран достъп до данни и ресурси;
- предотвратяване възможността за застрашаване целостта на информацията и наличните база данни в съда;
- предотвратяване възможно застрашаване конфиденциалността на компютърната мрежа на съда, в това число хардуера, софтуера, информацията и комуникационната инфраструктура;
- гарантиране ефикасното ползване на компютърната техника и наличен софтуер, работата с тях в съответствие с изпълнението на служебните задължения и само за тази цел.

1.3. 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 Наредбата за минималните изисквания за мрежова и информационна сигурност, приета с ПМС № 186 от 19.07.2019 г.

1.4. Настоящата политика се прилага и спазва задължително от всички потребители в съда при осигуряване на сигурността на информацията и са приложими по отношение на цялата компютърна и периферна техника, програмни продукти и бази данни.

2. Контрол на достъпа

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

- разделяне на потребителски от администраторски функции;
- установяване на нива и достъп до информация;

- регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;
- осъществяването на контрол от специализирани звена и служители на администрацията.

2.2. Достъпът до информация на персоналните компютри на работните места се осъществява, чрез предоставяне на валидно потребителско име и парола.

2.3. 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.

2.4. 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 оторизираното за това лице - системния администратор, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

2.5. Предоставянето на достъп става по дефиниран вътрешен ред, 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.

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

2.7. Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения обособени за целта в сградата на съда, съобразени с мерките за противопожарна защита.

2.8. Не се допускат външни лица до сървърите, с изключение на техници от оторизирани фирми, и то само придружени от съдебния или системния администратор.

2.9. Не се допуска достъпа на външни лица до компютърната техника в канцеларииите в сградата на съда.

2.10. На съдебните служители 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.

2.11. Съдебните служители са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до злоумишлен софтуер.

2.12. Съдът използва групова политика за заключване на профилите с password-protected screensaver, която се активира след липса на активност.

2.13. Всички пароли за достъп на системно ниво се променят периодично, спазвайки препоръките за сигурност с оглед осигуряване подходящо ниво на защита.

3. Работно място и правила за работа с носители на информация

3.1. Техниката на съда се ползва само за служебни цели.

3.2. Всеки съдебен 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.

3.3. Достъпът до данни от страна на съдебните служители се осъществява чрез въвеждане на потребителско име и парола.

3.4. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява системния администратор, който му оказва съответна техническа помощ.

3.5. Забраняват се опити за достъп до компютърна информация и бази данни, до които не са предоставени права, съобразно заеманата от съдебния служител длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп.

3.6. 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.

3.7. Не се позволява инсталирането на какъвто и да е нов или преконфигурирането от потребителите на вече инсталиран софтуер и хардуер, както и самостоятелни опити за поправка или подобрения на софтуер и хардуер. При съмнения за възникнал проблем незабавно се уведомява системния администратор.

3.8. Забранява се използването на внесени отвън преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на съда.

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

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

3.11. В края на работния ден всички компютри задължително се изключват.

4. Ползване на интернет

4.1. Достъпът до интернет и електронната поща е само за служебно ползване.

4.2. Забранява се съхраняването на сървърите на съда на лични файлове с текст, изображения, видео и аудио.

4.3. Забранява се отварянето без контрол от страна на системния администратор на:

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

5. Задължения на съдебните служители

5.1. Потребителите са длъжни да предприемат всички необходими мерки за предотвратяване на неоторизиран достъп до техниката и информацията на съда включително:

- защита на пароли и акаунти и забрана за тяхното споделяне;
- забранена за отваряне на прикачени към електронна кореспонденция файлове, получени от неизвестен източник;
- задължително изключване на компютрите в края на всеки работен ден;

5.2. На служителите в съда, които използват електронни бази данни и техни производни (текстове, разпечатки, дела, преписки и др.) се забранява:

- да ги изнасят под каквато и да е форма извън служебните помещения, освен с разрешение на председателя на съда;
- да ги използват извън рамките на служебните си задължения;
- да ги предоставят на външни лица без да е заявена услуга.

5.3. За нарушение целостта на данните се считат следните действия:

- унищожаване на бази данни или части от тях;
- повреждане на бази данни или части от тях;
- вписване на невярна информация в бази данни или части от тях.

6. Защита от компютърни вируси и друг зловреден софтуер

С цел антивирусна защита се прилагат следните мерки:

- всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява периодично;
- системният администратор извършва следните дейности:

-активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;

-настройва антивирусния софтуер за периодични сканирания на файловите системи на компютрите за вируси;

-активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система, освен в случаите когато работата с определени продукти или услуги на други институции не изискват различни настройки;

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

- при поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира системния администратор.

7. Осигуряване непрекъсваемост на работата

7.1. Всички сървъри и устройства за съхранение на данни трябва да са свързани към устройство за непрекъсваемост на електрическото снабдяване.

7.2. При срив в локалната компютърна мрежа, всеки потребител трябва 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.

10.02.2023г. **Председател на АдмС – Монтана:**

/Соня Камарашка/