

РАЙОНЕН СЪД - БОТЕВГРАД

2140 - град Ботевград, ул. „Свобода“, 3-Б тел./факс : 0723 69 344

e-mail: rajsud@abv.bg, web: www.rs-botevgrad.org

УТВЪРДИЛ:

Илияна Цветкова - Административен ръководител -
Председател на Районен съд - Ботевград



П РА В И Л А

ЗА ИЗПОЛЗВАНЕ НА ПРОГРАМНИ ПРОДУКТИ И ИНТЕРНЕТ В РАЙОНЕН СЪД - БОТЕВГРАД

Гр. Ботевград, 2010 г.

Целта на тези правила е:

- да се намали риска от неототоризиран достъп до данни и ресурси;
- да се предотврати възможно застрашаване цялостността, наличността и конфиденциалността на компютърната мрежа на съда, в това число софтуера, хардуера, информацията и комуникационната инфраструктура;
- да се гарантира, че потребителите ще използват ефикасно предоставената им компютърна техника и Интернет връзка в съответствие с изпълнението на служебните им задължения и само за тази цел.

Основни положения

Достъпът до Интернет, електронната поща и компютърното оборудване, осигурени от Районен съд - гр. Ботевград са само за служебно ползване. Използването им за лични цели е забранено.

Необходимо е да се спазват правилата относно използването на информацията и компютърното оборудване. Заобикалянето им под каквато и да е форма не е разрешено.

Всеки потребител носи собствена отговорност за действията си, независимо от действащите механизми за сигурност в тази насока.

Забранява се достъпа до компютърните файлове на други служители, освен личните. Разрешение за това дава съответния потребител, при наличието на основателна причина. За да се следи изпълнението на тези правила може да наложи извършването на мониторинг на компютрите. С цел осъществяване на техническата поддръжка може да се наложи преглед на съдържанието на файловете в компютрите. Това става с разрешението на ръководството на съда.

1. Вътрешна мрежа:

Достъп на потребителите - правила.

Всички тези правила помагат за по-добрата организация и по-ефективна работа с компютърната техника, за по-висока сигурност.

- Техниката да се използва изключително и само за служебни цели

- Логическият достъп на потребителите е подробно описан в създадените групови и индивидуални акаунти на сървър - домейн контролер. Той се определя от системния администратор на всеки съд, в зависимост от това с кои звена в организацията комуникира даденият потребител и какви мрежови приложения ползва.

За всеки потребител има регистрирани:

• Username (Име на потребителя) - уникално име на потребителя, избиращо се при регистрацията;

• Password (Парола) - необходимо е да отговаря на посочените по-долу изисквания;

• Full name (Пълно име) - пълното име на потребителя;

- Правата за достъп се определят в зависимост от това към коя логическа група принадлежи дадения потребител и с кои други такива трябва да комуникира в рамките на организацията, а също така и какви мрежови приложения използва при изпълнение на служебните си задължения.

- Не трябва да се използват общи акаунти за достъп до мрежовите ресурси и приложенията.

- Не трябва да се използват чужди акаунти за достъп до мрежовите ресурси и приложенията.

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

- Потребителите не трябва да извършват модификация на файл, който не е тяхна собственост, освен при наличието на основателни причини или чрез съгласието на собственика.

- Не се допускат външни лица до сървърното помещение, комуникационните шкафове, и техниката за интернет - връзка, с изключение на техници от ототоризирани фирми, и то само придружени от системния администратор.

- Единствено копие на ключовете до споменатите места има само системният администратор.

- Не се допуска достъпа на външни лица до компютърната техника в канцелариите в сградата на съда.

- В метална огнеупорна каса се съхраняват направените архивни копия.
- Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели.

Използване на лични пароли и персонална идентификация:

Защитата на информацията в системата е от огромно значение. За тази цел всеки служител има лична парола и персонална идентификация. Всеки потребител трябва да запази персоналната идентификация и лична парола и да не ги предоставя за използване от други лица.

- Паролите за достъп до системата трябва да отговарят на:

- Дължина на паролата минимум 6 /шест/ символа, от които един да бъде цифра, и поне една буква.

- Правата на крайният потребител и варира в зависимост от това как се използва ресурсите: права за писане и права за четене.

- Даденият достъп трябва да съдържа, от една страна, минимум привилегии, и от друга страна - да бъде достатъчен за адекватно изпълнение на служебните задължения на крайният потребител.

- В метална каса се съхраняват описаните по видове приложения пароли за достъп на всички потребители.

Инсталиране и конфигуриране на софтуер:

- 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. При съмнение за възникнал проблем незабавно се уведомява системният администратор.

- Не се позволява използването на внесени отвън информационни носители, както и внесени отвън софтуер и хардуер.

- Защитеният с авторски права и лицензиран софтуер не може да бъде копиран освен при изрично споменаване.

2. Използване на Интернет

Използването на неподходящи или обидни Интернет страници, като сайтове с непристойно съдържание, е забранено. Достъпът до Интернет става чрез браузъри, инсталирани от системния администратор. Потребителите трябва да имат, предвид че използването на Интернет и инсталирането на програми може да доведе до получаване на вируси.

Служителите не могат да използват Интернет връзката за гледане на видео или филми, които значително намаляват скоростта на връзката за другите служители.

Достъп на потребителите:

- Не се толерира влизането в Интернет - сайтове с неизвестно съдържание, или поне, ако въобще не предполагате какво съдържат те.

- Не е разрешено инсталирането и използването на чат - програми.

- Не е желателно тегленето на файлове с неизвестно съдържание от Интернет. Ако има нужда от това, се обръщайте към системния администратор.

- Не е желателно използването на активно съдържание, като ActiveX контроли и Java аплети, които позволяват по време на използването на Интернет в системата на потребителя да проникнат вируси или друг зловреден софтуер.

- Наличие на Интернет връзка има на следните компютри - Председател, съдии, системен администратор, административен секретар, бюро "Съдимост", счетоводител и секретар СИС.

- Забранено е използването на отдалечен достъп, FTP да се използва само за администраторски цели, през предварително зададен нестандартен порт. Достъп да имат само потребители със създадени акаунти и пароли на интернет-сървър.

Достъп и използване на електронната поща

- E-mail адресите в съда са само за служебна цел.

- Потребителят не бива да отваря съобщения, получени от неизвестен получател или неизвестна Интернет страница. Такива съобщения трябва да бъдат изтрети незабавно.

- Старите съобщения, които вече не са необходими с оглед изпълняването на служебните задължения, трябва да бъдат периодично изтривани. Потребителите трябва да преместват важната информация от получените съобщения в отделни файлове върху техните компютри.

3. Копирна и принтерна техника

Потребителите трябва да пазят принтерите, копирната и компютърна техника от физически увреждания. Външното почистване на техниката се извършва от потребителя като се използват само предназначените за целта консумативи и материали.

Не се допуска:

- Поставянето на предмети върху принтери и копирна техника, което създава предпоставки за физическото им увреждане.
- Самостоятелни опити за поправка на принтери и копирна техника. При съмнение за съществуващ проблем се обръщайте към системния администратор.
- Работата на външни лица с наличната копирна и принтерна техника, както и техни опити за отстраняване на възникнали проблеми, освен на лица – служители на оторизираните за това фирми, със знанието на системния администратор.
- Смяната на тонер-касети и отстраняването на заседнали листи да се извършва на място, само от обучени за това служители или от системния администратор.
- Копиране или отпечатване на материали нямащи връзка с изпълнението на служебните задължения.

Следните дейности са строго забранени:

1. Опити за неоторизиран достъп до компютърната система.
2. Извършването на дейности, които застрашават целостта на компютърната мрежа.
3. Предоставяне на пароли за достъп до компютърната система или мрежа на външни лица.
4. Използването на чуждо потребителско име, парола и електронна поща.
5. Използването на компютърни игри през работно време.
6. Инсталирането на софтуер, както и инсталирането на нелегален софтуер, използването на авторски материали без разрешение, както и всякакви други дейности, които нарушават авторските права.
7. Повредата или разрушаването на компютърното оборудване, софтуер или информация.

Изготвил:


Станислав Йотов – Системен администратор