BenchMark
est. 2003

ПРАВИЛА ЗА ИНФОРМАЦИОННА СИГУРНОСТ НА ЛИЧНИТЕ ДАННИ

I. Общи положения

Настоящите правила се приемат с цел защита и контрол на компютърните и информационните системи на инвестиционния посредник, както и за осигуряване на защита на данните и информацията за клиентите, съхранявана при инвестиционния посредник. Правилата са насочени към поддържане на надеждни системи и мрежи, осигуряване на високо ниво на сигурност, предоставяне на достъп според заемната длъжност и функция, извършване на постоянен контрол и навременна актуализация на използваните софтуерни продукти.

Работата, 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 от специализирани звена и служители на посредника.

II. Поддържане и защита на информационните и компютърните системи

Инвестиционният посредник има самостоятелен отдел Информационни технологии (IT Отдел), чиито основни функции са следните:

1. Подготвя и инсталира необходимите компютърни системи (хардуер) и софтуер;
2. Оказва методическа помощ на служителите при работата им с компютърните системи и софтуер;
3. Извършва оценка и одобрение на използвания софтуер и хардуер, включително на подбора на доставчици на интернет и информационни услуги;
4. Разработва, внедрява и поддържа системи за препятстване и контрол на нерегламентиран достъп до информация и бази данни;
5. Внедрява и поддържа антивирусен софтуер;
6. Разработва, внедрява и поддържа системи за авторизация и идентификация при влизане и излизане от компютърните системи;
7. Разработва план за действие при извънредни ситуации за запазване на компютърните и информационните системи и за възстановяване на тяхното нормално функциониране.

III. Права и задължения на служителите на инвестиционния посредник по отношение на информационните и компютърните системи

Лицата, работещи по договор с Инвестиционния посредник, са длъжни да спазват следните общи правила при работата с компютърни и информационни системи:

1. Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола;
2. Забранява се предоставянето на трети лица на личното потребителско име и паролата за влизане в служебния компютър;
3. След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off;
4. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Системния администратор, който му оказва съответна техническа помощ;
5. 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;
6. Забранява се инсталирането и използването на незаконен софтуер.
7. Забранява се изнасянето на хардуер или носители на информация, които съдържат лични данни.
8. 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.
9. 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."
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.
11. Въведени са конкретни мерки за защита на информационните и компютърните системи срещу компютърни вируси, срив на локалните мрежи, прекъсване на електрозахранването и др., както следва:

IV. Защита от компютърни вируси и друг зловреден софтуер

Следните мерки се прилагат с цел антивирусна защита:

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

2. Системният администратор извършва следните дейности:

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

   2.2. настройва антивирусния софтуер за периодични сканирания през определен период, но поне веднъж седмично.

   2.3. активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система;

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

3. При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира Системния администратор.

V. Непрекъснатост на работата

Следните мерки се прилагат при срив на локалната мрежа:

1. Всички персонални компютри са свързани към устройство за непрекъсваемост на ел. снабдяването.

2. При срив на ел. мрежа всички служители са длъжни незабавно да запишат всички файлове, които са отворили на сървърите и да прекратят работата си.

3. При липса на ел. захранване за повече от 10 мин., Системният администратор започва процедура по поетапно спиране на сървърите.

4. При срив 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. Резервиране

Информацията, включително тази, съдържаща лични данни, се резервира по следния начин:

1. Автоматизирано и планово се извършва резервиране на цялата работна информация на сървърите и дисковите масиви.
2. Резервирането 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 Eurosys Системата се резервират всяка вечер;
4. Споделените документи се резервират 2 пъти седмично.

VII. Контрол на достъпа и правила за работа с носители

Прилагат се следните мерки за защитено влизане в системата:

1. Всеки служител има точно определени права на достъп и използва уникален потребителски ID за вход в системата и достъп до директорията, до която е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови ID;

2. 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 Системния администратор, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

3. Предоставянето на достъп става по дефиниран вътрешнофирмен 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.

4. Системният администратор незабавно отменя правата за достъп на лица, които вече не са служители;

5. Системният администратор извършва текуща проверка за премахване или блокиране на излишните ID и акаунти и не предоставя излишните потребителски ID на други потребители;

6. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн;

7. Всички пароли за достъп на системно ниво се променят периодично;

8. Мейли, съдържащи чувствителна информация или лични данни, се изпращат през криптирана връзка.

9. 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.

10. При изнасяне на носители извън физическите граници на офиса на дружеството, те се поставят в подходяща опаковка и в запечатан плик. На служителите 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.

11. 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.

12. 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.

VIII. Заключителни разпоредби

Настоящата политика се разглежда и оценява периодично с оглед ефективността ѝ, като инвестиционният посредник може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

Настоящата политика се предоставя за сведение и изпълнение на служителите, като Съветът на директорите може да издава заповеди и инструкции относно нейното прилагане.