ООО «АКСИС Менеджмент»
105066, Москва, ул. Н. Красносельская, 35с64,
БЦ «Виктория Плаза» +7 495 665 2250
info@axes.ru www.axes.ru

Политика информационной безопасности в ООО «АКСИС Менеджмент»

1. Общие положения

1.1. Настоящая Политика разработана в соответствии с действующим законодательством, нормативными актами и соотносимыми с ними положениями внутренних документов ООО «АКСИС Менеджмент» (далее – Компания). Она регламентирует порядок обеспечения сохранности информации и ее безопасности в Компании как в осуществлении текущей деятельности, так и в обозримом будущем.

1.2. Предметом настоящего документа является:

- порядок доступа к конфиденциальной информации;
- работа с криптографическими системами;
- физическая безопасность (доступ в помещения);
- разграничение прав доступа;
- работа в глобальной сети Интернет;
- дублирование, резервирование и раздельное хранение конфиденциальной информации.

1.3. В настоящей Политике под термином «сотрудник» понимаются все сотрудники Компании. На лиц, работающих в Компании по договорам гражданско-правового характера, в том числе прикомандированных, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре.

1.4. Ответственность за соблюдение информационной безопасности несет каждый сотрудник Компании.

1.5. Каждый новый сотрудник проходит обучение принципам безопасного использования платформы. По результатам обучения все сотрудники проходят срез знаний в виде теста. Данный срез знаний является определяющим для дальнейшей работы сотрудника в Компании.

1.6. Обновление платформы проходит не реже раза в месяц.

2. Порядок доступа к конфиденциальной информации

2.1. В целях обеспечения защиты информации в Компании, устанавливается следующий порядок допуска к работе с конфиденциальными источниками:

- Решение о доступе работника к определенному разделу клиентской информации принимается руководством Компании.
- Отдел информационных технологий обеспечивает защиту отдельных файлов и программ от чтения, удаления, копирования лицами, не допущенными к этому.
- Доступ к компьютерной сети Компании осуществляется только с персональным паролем. Пользователь должен держать в тайне свой пароль. Сообщать свой пароль другим лицам, а также пользоваться чужими паролями запрещается.

ООО «АКСИС Менеджмент»
105066, Москва, ул. Н. Красносельская, 35с64,
БЦ «Виктория Плаза» +7 495 665 2250
info@axes.ru www.axes.ru

2.2. Категорически запрещается снимать несанкционированные копии с носителей клиентской и иной внутренней информации, знакомить с содержанием электронной информации лиц, не допущенных к этому.

2.3. Доступ третьих лиц к информационным системам Компании строго запрещен.

2.4. Каждый сотрудник обязан немедленно уведомить руководителя Отдела информационных технологий и руководство Компании обо всех случаях несанкционированного получения доступа третьими лицами к ресурсам корпоративной сети.

2.5. Сотрудникам, использующим в работе портативные компьютеры Компании, может быть предоставлен удаленный доступ к сетевым ресурсам Компании в соответствии с правами в корпоративной информационной системе.

2.6. Сотрудникам, работающим за пределами Компании с использованием компьютера, не принадлежащего Компании, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

2.7. Сотрудники и третьи лица, имеющие право удаленного доступа к информационным ресурсам Компании, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Компании и к каким-либо другим сетям, не принадлежащим Компании.

2.8. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Компании, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

3. Работа с криптографическими системами

3.1. К работе с криптографическими системами допускаются только сотрудники Компании, имеющие соответствующее разрешение от руководства Компании.

3.2. Секретные ключи электронно-цифровых подписей и шифрования должны храниться в сейфах под ответственностью лиц на то уполномоченных. Доступ неуполномоченных лиц к носителям секретных ключей и шифрования должен быть исключен.

3.3. Категорически запрещается:

— выводить секретные ключи и шифрования на дисплей компьютера или принтер;
— устанавливать в дисковод компьютера носитель секретных ключей и шифрования в непредусмотренных режимах функционирования;
— записывать на носитель секретных ключей и шифрования постороннюю информацию.

3.4. При компрометации секретных ключей, шифрования и прочей электронной информации Отделом информационных технологий принимаются меры для прекращения любых операций с использованием этих ключей и прочей информации; принимаются меры для смены ключей и шифрования, паролей. По факту компрометации организуется служебное расследование, результаты которого отражаются в акте и доводятся до сведения руководства Компании.

ООО «АКСИС Менеджмент»
105066, Москва, ул. Н. Красносельская, 35с64,
БЦ «Виктория Плаза» +7 495 665 2250
info@axes.ru www.axes.ru

4. Физическая безопасность

4.1. Все объекты, критичные с точки зрения информационной безопасности (все сервера баз данных, телефонная станция, основной маршрутизатор, файрволл), находятся в отдельном помещении, доступ в которое разрешен только сотрудникам, имеющим соответствующее разрешение от руководства Компании.

4.2. Помещение оборудовано принудительной вентиляцией и пожарной сигнализацией. Вход в помещение контролируется системой видео наблюдения.

4.3. Ключевые дискеты, пароли и прочая конфиденциальная информация хранится в сейфах.

4.4. Доступ в помещение в неурочное время или в выходные и праздничные дни осуществляется строго по индивидуальным пропускам.

5. Разграничение прав доступа к программному обеспечению и системам хранения данных

5.1. Для входа в компьютерную сеть Компании сотрудник должен ввести имя и пароль. Не допускается режимы беспарольного (гостевого) доступа к какой-либо внутренней информации.

5.2. В целях защиты конфиденциальной информации Компании организационно и технически разделяются сотрудники Компании, имеющие доступ и работающие с различной информацией (в разрезе ее конфиденциальности и смысловой направленности).

Данная задача решается с использованием сетевых ресурсов и папок с возможностью предоставления разных уровней доступа и сетевой операционной системы, где в целях обеспечения защиты данных доступ и права пользователей ограничиваются персональными каталогами. Права назначаются в соответствии с производственной необходимостью, определяемой начальником подразделения.

5.3. Параметры входа в сеть, имя и пароль, пользователем не разглашаются. Копии на бумажном носителе держатся в недоступном для посторонних месте. В случае компрометации пароля пользователь должен незамедлительно обратиться в Отдел информационных технологий с заявкой о замене.

6. Работа в глобальной сети Интернет

6.1. К работе с ресурсами сетью Интернет допускаются сотрудники, получившие соответствующее разрешение от руководства Компании (достаточна устная форма).

6.2. При работе с сетью Интернет сотрудникам запрещено:

— Самостоятельно (без одобрения администратора сети) скачивать и устанавливать на компьютер программное обеспечение.
— Посещать ресурсы, не имеющие непосредственного отношения к работе и служебным обязанностям.
— Осуществлять подписку на рассылку информации непроизводственного характера.

ООО «АКСИС Менеджмент»
105066, Москва, ул. Н. Красносельская, 35с64,
БЦ «Виктория Плаза» +7 495 665 2250
info@axes.ru www.axes.ru

— Сообщать адрес электронной почты в непроизводственных целях.
— Пользоваться различными Интернет-пейджерами.
— Использовать Интернет для получения материальной выгоды или непроизводственных целях, в том числе осуществляя торговлю через Интернет.

7. Дублирование, резервирование и раздельное хранение конфиденциальной информации

7.1. В целях защиты внутренней информации от преднамеренного или же непреднамеренного ее уничтожения, фальсификации или разглашения сотрудники Отдела информационных технологий контролируют обеспечение

— ежедневного обязательного резервирования всей клиентской информации, содержащейся на платформах Компании и имеющей конфиденциальный характер,
— дублирования информации с использованием различных физических и аппаратных носителей.

7.2. Ответственность за хранение и резервирование внутренней информации на серверах Компании возлагается на Отдел информационных технологий.

7.3. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на сотрудниках. Специалисты Отдела информационных технологий обязаны оказывать сотрудникам содействие в проведении резервного копирования данных на соответствующие носители.

7.4. Только специалисты Отдела информационных технологий на основании заявок руководителей подразделений могут создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

7.5. Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

8. Сканирование уязвимостей

8.1. Сканирование уязвимостей узлов информационной сети Организации проводится один раз в квартал.

8.2. Внеплановому сканированию подлежат:

— новые узлы, впервые подключаемые к информационной сети Организации;
— существующие узлы, на которых была произведена переустановка операционной системы, либо установлены комплексные обновления ОС и(или) прикладного программного обеспечения, осуществляющего сетевое взаимодействие;
— существующие узлы, на которых была произведена смена версии прикладного программного обеспечения, осуществляющего сетевое взаимодействие;
— узлы (группы узлов), на которых была обнаружена или заподозрена вирусная активность;

ООО «АКСИС Менеджмент»
105066, Москва, ул. Н. Красносельская, 35с64,
БЦ «Виктория Плаза» +7 495 665 2250
info@axes.ru www.axes.ru

— узлы, использующие программное обеспечение, для которого в общедоступных источниках была опубликована критическая уязвимость.

8.3. Для новых узлов, при типовом наборе программного обеспечения данного узла (для данного набора программного обеспечения уже проводилось сканирование уязвимостей), либо существующих узлов при установке версии операционной системы и версий и (или) обновлений программного обеспечения для которых ранее проводилось плановое сканирование, возможно проведение сканирования без определения уязвимостей – сканирование портов.

8.4. Проведение сканирования нового узла должно производиться до момента его подключения в информационную сеть Организации.

8.5. Отдел информационных технологий производит анализ обнаруженных в ходе сканирования уязвимостей, на предмет степени критичности данной уязвимости для функционирования информационной системы и возможных последствий при использовании данной уязвимости злоумышленником.

8.6. На основании результатов анализа отделом информационной безопасности производится дополнительная проверка выявленных уязвимостей и, в случае подтверждения результатов, полученных в ходе сканирования, установка обновлений, исправляющих данную уязвимость, в случае их наличия у разработчика, либо передача информации об уязвимости разработчику программного обеспечения, в котором данная уязвимость была обнаружена.

8.7. После установки обновления, устраняющего найденную уязвимость, необходимо проведение повторного, внепланового, сканирования данного узла.

8.8. В случае отсутствия у разработчика программного обеспечения необходимого обновления, устраняющего найденную критическую уязвимость, отделом информационной безопасности разрабатываются мероприятия, снижающие риск использования данной критической уязвимости. В том числе возможно проведение попыток практической реализации атаки, использующей найденную уязвимость.

8.9. В качестве дополнительной проверки возможности практического использования злоумышленником найденных критических уязвимостей, для которых не существует обновлений, устраняющих их, может привлекаться специализированная организация, для осуществления тестов на проникновение.

8.10. В целях обеспечения стабильного и бесперебойного функционирования информационной сети при проведении сканирования запрещается одновременное сканирование более 20-ти сетевых узлов, а также применение настроек разрешающих использование найденных уязвимостей и проверок, потенциально способных привести к нарушению работоспособности сканируемого узла. При проведении сканирования с использованием потенциально опасной конфигурации сканера безопасности необходимо уведомить администратора информационной системы и проводить сканирование с присутствием администратора данной информационной системы.

ООО «АКСИС Менеджмент»
105066, Москва, ул. Н. Красносельская, 35с64,
БЦ «Виктория Плаза» +7 495 665 2250
info@axes.ru www.axes.ru

8.11. Перед проведением сканирования, произвести резервное копирование информации необходимой для восстановления работоспособности приложения (узла), а в случае изменения данной информации в режиме реального времени и отсутствия возможностей восстановления информации, проводить сканирование в моменты, когда данная информация изменяется (пополняется) с наименьшей скоростью.

8.12. Проводить сканирование в присутствии администратора данного приложения, для обеспечения возможности максимально быстрого восстановления работоспособности данного приложения.

8.13. Лог файлы, полученные в ходе проведения сканирования уязвимостей, а также информация об обнаруженных уязвимостях является конфиденциальной информацией. Полный доступ к информации, полученной в ходе сканирования, предоставляется сотрудникам отдела информационной безопасности и руководству Организации.

8.14. Доступ к информации, полученной в ходе проведения сканирования, может быть предоставлен сотрудникам ответственным за сопровождение прикладных систем, в которых обнаружены уязвимости, но только в части информации, имеющей непосредственное отношение к сопровождаемым системам.

8.15. Допускается предоставление информации об обнаруженных уязвимостях в программном обеспечении, разработчикам данного программного обеспечения, при этом разработчику предоставляется только та часть информации о уязвимостях, которая имеет непосредственное отношение к данному программному обеспечению.

8.16. При привлечении сторонней организации для проведения тестирования на проникновение необходимо заключение договора, предусматривающего обязательное соблюдение конфиденциальности информации предоставленной данной Организации, а также информации, собранной в ходе выполнения работ и результатов их выполнения.

9. Реагирование на инциденты

9.1. Источником информации об инциденте информационной безопасности может служить следующее:

- сообщения сотрудников, клиентов, контрагентов Компании, направленные в Компанию виде сообщений по электронной почте, служебных записок, писем, заявлений и т.д.
- данные, полученные на основании анализа журналов регистрации информационных систем, систем защиты.

9.2. При получении сообщения об инциденте информационной безопасности по электронной почте или по телефонному звонку необходимо убедиться в достоверности полученной информации (например, путем совершения «обратного» звонка по указанным в сообщении телефонам, проверки данных, указанных в подписи сообщения или названных при звонке).

9.3. Сотрудник, получивший информацию об инциденте, должен сообщить об этом в Отдел информационной безопасности и начальнику подразделения, в котором случился инцидент.

ООО «АКСИС Менеджмент»
105066, Москва, ул. Н. Красносельская, 35с64,
БЦ «Виктория Плаза» +7 495 665 2250
info@axes.ru www.axes.ru

9.4. Отдел информационных технологий собирает и анализирует все данные об обстоятельствах инцидента (электронные письма, логи информационных систем, показания сотрудников и др.).

9.5. Отдел информационных технологий обязан установить, имела ли место утечка сведений, и обстоятельства, ей сопутствующие, установить лица, виновные в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению.

Подпись уполномоченного лица

Львов С. Ю.

Генеральный директор
ООО «АКСИС Менеджмент»