**Политика информационной безопасности**

**Компания ООО “Василёк”.**

**Штат - 103 сотрудников**.

10 - руководство

15 - бухгалтерия

20 – IT-отдел

40 - менеджеры по работе с клиентами

18 - отдел информационной безопасности

Руководство копании использует телефонную связь, MS Office, 1C:Предприятие и т.д.

Бухгалтерия использует телефонную связь, MS Office, 1C:Бухгалтерия.

IT-отдел обеспечивает функционирование внутренних сетей организации, а также сайта компании и личных кабинетов клиентов.

Менеджеры по работе с клиентами осуществляют работу с ними посредством Интернет. Телефонной связи

1. **Термины и определения**

Риск — возможность возникновения финансовых потерь (убытков), незапланированных расходов или возможность снижения планируемых доходов.

· Операционные риски — это риски, связанные с финансово-экономической деятельностью (без учета рыночных и кредитных рисков), потери по которым связаны с результатами некомпетентного управления человеческими, технологическими факторами или внешними событиями.

· Служба автоматизации — Департамент ИТ и отдельные сотрудники, ответственные за обеспечение IT-сервиса (в том числе и организации, выполняющие данные работы по договору).

· Автоматизированная система обработки информации (АС) — организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей государственных органов, коммерческих или некоммерческих организаций (юридических лиц), граждан (физических лиц) и иных потребителей информации.

· Информационные средства — средства, предназначенные для хранения, обработки и передачи компьютерной информации, а именно: компьютеры и комплексы, терминалы доступа к ним, оборудование локальных вычислительных сетей и узлов связи, специальное оборудование на основе компьютеров, криптографическое оборудование.

· Информационный актив — различные виды информации (платежной, финансово-аналитической, служебной, управляющей, справочной и пр.) на всех этапах ее жизненного цикла, обеспечивающей деятельность и представляющей ценность с точки зрения достижения поставленных бизнес-целей.

· Владелец информационного актива — структурное подразделение, отдел, служба, реализующее полномочия владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Владелец информационного актива определяется на этапе его создания.

· Информация — это сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (об их свойствах, характеристиках) в некоторой предметной области, необходимые для оптимизации принимаемых решений в процессе управления данными объектами.

· Инцидент информационной безопасности — действительное, предпринимаемое или вероятное нарушение информационной безопасности.

Нарушение может быть вызвано ошибками персонала, неправильным функционированием технических средств, природными факторами, преднамеренными злоумышленными действиями, приводящими к нарушению доступности, целостности, конфиденциальности информации.

· Firewall (межсетевой экран) — программно-аппаратный комплекс, применяемый для разграничения доступа между сетями.

· Доступ к информации — ознакомление с информацией, ее обработка, в частности: копирование, модификация или уничтожение информации.

· Санкционированный доступ к информации — доступ к информации, не нарушающий правила разграничения доступа.

· НСД (Несанкционированный доступ к информации) — доступ к информации, нарушающий правила разграничения доступа.

1.1 **Цель и назначение настоящей политики**

Доступность информации — свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

· Целостность информации — свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

· Конфиденциальность информации — субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

2. **Общие положения**

Настоящая политика информационной безопасности предусматривает принятие необходимых мер в целях защиты активов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Компании.

С целью минимизации рисков отдел информационной безопасности обеспечивает выполнение требований целостности, конфиденциальности и доступности информации.

Все далее указанные требования обязательны к исполнению всеми работниками структурных подразделений, отделов и служб.

Все требования по обеспечению информационной безопасности применимы к каждому работнику, а также к любому третьему лицу, включая лиц, работающих по договорам гражданско-правового характера и прикомандированных работников, имеющих доступ к информации и ее информационным ресурсам.

Каждый работник, а также любое третье лицо, включая лиц, работающих по договорам гражданско-правового характера и прикомандированных работников, имеющих доступ к информации и ее информационным ресурсам признает право на осуществление контроля их деятельности при работе с информационными средствами и информацией.

Вся деловая информация в любой форме, приобретенная или полученная, используемая для поддержки его законной производственно-хозяйственной деятельности, либо разработанная его работниками в ходе производственно-хозяйственной деятельности, принадлежит Организации. Это право собственности распространяется на голосовую и факсимильную связь с использованием аппаратуры, на лицензионное и разработанное программное обеспечение и отдельные программы, на электронные почтовые ящики, а также на бумажные и электронные файлы всех бизнес-направлений, бизнес-функций, и на всех работников.

Запрещается использование информации и информационных средств в личных целях.

### 3. **Цель и назначение настоящей Политики**

**Целями настоящей Политики являются:**

* сохранение конфиденциальности критичных информационных ресурсов;
* обеспечение непрерывности доступа к информационным ресурсам Компании для поддержки бизнес деятельности;
* защита целостности деловой информации с целью поддержания возможности Компании по оказанию услуг высокого качества и принятию эффективных управленческих решений;
* повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Компании;
* определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Компании.

Руководители подразделений Компании должны обеспечить регулярный контроль за соблюдением положений настоящей Политики. Кроме того, должна быть организована периодическая проверка соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки Руководству.

4. **Требования и рекомендации защиты информации**

### 4.1. **Ответственность за информационные активы**

В отношении всех собственных информационных активов Компании, активов, находящихся под контролем Компании, а также активов, используемых для получения доступа к инфраструктуре Компании, должна быть определена ответственность соответствующего сотрудника Компании.

Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами Компании должна доводиться до сведения руководителя Департамента информационных технологий и руководителя Департамента защиты информации Компании.

### 4.2. **Контроль доступа к информационным системам**

#### 4.2.1. **Общие положения**

Все работы в пределах офисов Компании выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Компании.

Внос в здания и помещения Компании личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы Компании производится только при согласовании с Департаментом защиты информации Компании.

Все данные (конфиденциальные или строго конфиденциальные), составляющие коммерческую тайну Компании и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы. Все портативные компьютеры Компании должны быть оснащены программным обеспечением по шифрованию жесткого диска.

Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

В процессе своей работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.

#### 4.2.2. **Доступ третьих лиц к системам Компании**

Каждый сотрудник обязан немедленно уведомить руководителя Департамента информационных технологий и руководителя Департамента защиты информации обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

Доступ третьих лиц к информационным системам Компании должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам Компании должен быть четко определен, контролируем и защищен.

#### 4.2.3. **Удаленный доступ**

Пользователи получают право удаленного доступа к информационным ресурсам Компании с учетом их взаимоотношений с Компанией.

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

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

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.

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

#### 4.2.4. **Доступ к сети Интернет**

Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила:

* сотрудникам Компании разрешается использовать сеть Интернет только в служебных целях;
* запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;
* сотрудники Компании не должны использовать сеть Интернет для хранения корпоративных данных;
* работа сотрудников Компании с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Компании в сеть Интернет;
* сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Компании;
* сотрудники Компании перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
* запрещен доступ в Интернет через сеть Компании для всех лиц, не являющихся сотрудниками Компании, включая членов семьи сотрудников Компании.

Специалисты Департамента информационных технологий и Департамента защиты информации имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

### 4.3 **Защита оборудования**

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранятся информация Компании.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят авторизованные специалисты Департамента информационных технологий, после согласования изменений с Департаментом защиты информации.

#### 4.3.1. **Аппаратное обеспечение**

Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для СD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей Политики вместе именуются «компьютерное оборудование». Компьютерное оборудование, предоставленное Компанией, является ее собственностью и предназначено для использования исключительно в производственных целях.

Пользователи портативных компьютеров, содержащих информацию, составляющую коммерческую тайну Компании, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах, или обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства, в случаях, когда данный компьютер не используется.

Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности, как в офисе, так и по месту проживания. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например, в гостиницах, аэропортах, в офисах деловых партнеров и т.д., пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра.

Во время поездки в автомобиле портативный компьютер должен находиться в багажнике. На ночь его следует перенести из автомобиля в гостиничный номер.

Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавише и после выхода из режима «Экранной заставки». Для установки режимов защиты пользователь должен обратиться в службу технической поддержки. Данные не должны быть скомпрометированы в случае халатности или небрежности, приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

При записи какой-либо информации на носитель для передачи его контрагентам или партнерам по бизнесу необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

Карманные персональные компьютеры, а также мобильные телефоны, имеющие функцию электронной почты и прочие переносные устройства, не относятся к числу устройств, имеющих надежные механизмы защиты данных. В подобном устройстве не рекомендуется хранить конфиденциальную информацию.

Порты передачи данных, в том числе FD и CD дисководы в стационарных компьютерах сотрудников Компании блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись информации у Департамента защиты информации.

#### 4.3.2. **Программное обеспечение**

Все программное обеспечение, установленное на предоставленном Компанией компьютерном оборудовании, является собственностью Компании и должно использоваться исключительно в производственных целях.

Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственному руководителю сотрудника и в Департамент защиты информации.

На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

* персональный межсетевой экран;
* антивирусное программное обеспечение;
* программное обеспечение шифрования жестких дисков;
* программное обеспечение шифрования почтовых сообщений.

Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной руководителем Департамента информационных технологий.

Сотрудники Компании не должны:

* блокировать антивирусное программное обеспечение;
* устанавливать другое антивирусное программное обеспечение;
* изменять настройки и конфигурацию антивирусного программного обеспечения.

Компания предпочитает приобретать программное обеспечение, а не разрабатывать собственные программы, поэтому пользователям, желающим внедрить новые возможности бизнес-процессов, необходимо обсудить свое предложение со своим менеджером по бизнес информации, который проинформирует их о порядке приобретения и/или разработки программного обеспечения.

### 4.7. **Управление сетью**

Уполномоченные сотрудники Департамента информационных технологий и Департамента защиты информации контролируют содержание всех потоков данных проходящих через сеть Компании.

Сотрудникам Компании запрещается:

* нарушать информационную безопасность и работу сети Компании;
* сканировать порты или систему безопасности;
* контролировать работу сети с перехватом данных;
* получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
* использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
* передавать информацию о сотрудниках или списки сотрудников Компании посторонним лицам;
* создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

#### 4.7.1. **Защита и сохранность данных**

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях. Специалисты Департамента информационных технологий обязаны оказывать пользователям содействие в проведении резервного копирования данных на соответствующие носители.

Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

Только специалисты Департамента 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.

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.

Все заявки на проведение технического обслуживания компьютеров должны направляться в Департамент информационных технологий.

### 4.8. **Разработка систем и управление внесением изменений**

Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, согласованны с руководителями Департамента защиты информации и Департамента информационных технологий.