Жилищный накопительный кооператив "ЦЕНТР БЕЗОПАСНОЙ ПОКУПКИ ЖИЛЬЯ"

ПОЛОЖЕНИЕ
об информационной безопасности
ЖНК «Центр безопасной покупки жилья»

Утверждаю
Директор ЖНК «Центр безопасной покупки жилья»

Пороцкий К.Ю.
11.01.2016

Настоящее Положение разработано в соответствии с разделом VII части 4 ГК РФ, ТК РФ, ФЗ «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006г., ФЗ «О коммерческой тайне» № 98 ФЗ от 29.07.2004г., ФЗ «О персональных данных» №152-ФЗ от 27.07.2006г. с целью организации и систематизирования деятельности, направленной на обеспечение информационной безопасности ЖНК «Центр безопасной покупки жилья»
(далее-Компания).

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В настоящем документе используются следующие основные понятия:

1.1.1. **Информационная безопасность** – условия, обеспечивающие целостность, доступность и конфиденциальность информации, а также защищённость информации и поддерживающей инфраструктуры от способных нанести ущерб её владельцам и пользователям неблагоприятных и несанкционированных воздействий случайного или преднамеренного характера, естественного или искусственного происхождения.

1.1.2. **Информация - сведения** (сообщения, данные) независимо от формы их представления (устной, письменной, в том числе с использованием технических средств).

1.1.3. **Коммерческая тайна** - режим конфиденциальности информации, позволяющий защитить информацию, имеющую действительную или потенциальную коммерческую ценность в силу.

1.1.4. **Служебная тайна** - режим конфиденциальности информации, позволяющий защитить информацию, имеющую действительную или потенциальную ценность в соответствии с федеральным законодательством и корпоративными положениями, настоящим Положением или в силу ее неизвестности третьим лицам от незаконного использования или разглашения третьим лицам.

1.1.5. **Конфиденциальность** - обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия обладателя исключительных прав.

1.1.6. **Предоставление информации** - действия, направленные на получение информации определённым кругом лиц или передачу информации определённому кругу лиц.

1.1.7. **Распространение информации** - действия, направленные на получение информации неопределённым кругом лиц или передачу информации неопределённому кругу лиц.

1.1.8. **Целостность** - свойство информации, указывающее, что информация не подверглась несанкционированной модификации или несанкционированному уничтожению.

1.1.9. **Доступность** - свойство информации, обеспечивающее беспрепятственный доступ к ней определённого круга лиц для проведения санкционированных операций по ознакомлению, документированию, модификации и уничтожению.

1.1.10. **Носители информации (в т.ч. коммерческой тайны):**

- автоматизированные системы и телекоммуникационные сети различного назначения, в которых информация обрабатывается, хранится и передаётся;
- материальные носители (бумажные, магнитные, оптические носители, чипы), в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- сотрудники, в т.ч. сотрудники, допущенные к сведениям, составляющим коммерческую тайну;
-контрагенты, третьи лица, допущенные к некоторым сведениям, составляющим коммерческую тайну;

1.1.11. **Документированная информация (документ)** - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

1.1.12. **Допуск к коммерческой тайне** - процедура оформления доступа сотрудников и третьих лиц к сведениям, составляющим коммерческую тайну;

1.1.13. **Доступ к сведениям, составляющим коммерческую тайну** - санкционированное Директором Компании ознакомление сотрудников со сведениями, составляющими коммерческую тайну.

1.1.14. **Гриф конфиденциальности** - штамп, визуально свидетельствующий о статусе конфиденциальности сведений, содержащихся на их носителе, проставляемый на самом носителе и (или) в сопроводительной документации к нему;

1.1.15. **В Компании устанавливаются следующие грифы конфиденциальности:**

а) **«коммерческая тайна»** в соответствии с Перечнем сведений, составляющих коммерческую тайну Компании;

б) «**ДСП**» - для служебного пользования» в соответствии с Перечнем сведений, составляющих служебную тайну Компании;

в) «**ИОД**» - информация ограниченного доступа» - в строгом соответствии с Перечнем лиц, указанным для ознакомления в самом документе.

г)**«ПД»** - персональные данные» - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Информация, содержащая персональные данные может быть с грифом «ПД-ДСП» и «ПД-ИОД».

1.1.16. **Перечень сведений, составляющих коммерческую тайну** - совокупность категорий сведений, в соответствии с которыми сведения относятся к коммерческой тайне Компании и охраняются на основаниях и в порядке, установленных федеральным законодательством;

1.1.17. **Перечень сведений, составляющих служебную тайну Компании** - совокупность сведений, в соответствии с которыми сведения относятся к служебной тайне Компании и охраняются на основаниях и в порядке, установленных федеральным законодательством и настоящим Положением;

1.1.18. **Перечень сведений, составляющих персональные данные работников Компании** - в соответствии со ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и

место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, сведения о занимаемой должности и размере заработной платы работника и т.д.

1.1.19. Перечни сведений, указанных в п.п. 1.1.15 и 1.1.16 настоящего Положения утверждаются и корректируются Приказами Директора Компании.

1.1.20. **Утечка информации** - неконтролируемое и несанкционированное распространение защищаемой в соответствии с Законом и настоящим положением информации.

1.1.21. **Разглашение коммерческой тайны** - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия правообладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

1.1.22. **Утрата документов или материальных носителей, содержащих сведения, относящиеся к коммерческой тайне** - выход (в том числе и временный) документов или материальных носителей из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы или материальные носители стали, либо могли стать достоянием посторонних лиц;

1.1.23. **Любое несанкционированное правообладателем копирование и разглашение информации, составляющей коммерческую тайну, между авторами, пользователями и иными лицами, допущенными к использованию сайтов Компании, расценивается как кража информации (интеллектуальной собственности компании) и влечёт уголовную и имущественную ответственность.**

1.1.24. **Идентификация** — присвоение пользователю и объекту доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

1.1.25. **Аутентификация** — проверка принадлежности пользователя предъявленным им идентификаторам, подтверждение подлинности.

2. ЦЕЛИ И ЗАДАЧИ

2.1. Главной целью информационной безопасности является обеспечение устойчивого функционирования Компании, защита информационных ресурсов и исключительных прав на интеллектуальную собственность, принадлежащих Компании, её пайщикам, партнерам, инвесторам, членам, клиентам от случайных (ошибочных) и направленных противоправных посягательств, разглашения, утраты, утечки, искажения, модификации и уничтожения охраняемых сведений.

2.2. Целями Положения являются:

2.3. - формирование целостного представления об информационной безопасности и взаимосвязь ее с другими элементами системы безопасности Компании;

2.4. - определение основных принципов реализации мероприятий, обеспечивающих необходимый уровень информационной безопасности.

2.5. 2.3. Задачами информационной безопасности Компании являются:

2.6. - обеспечение охраны информации и объектов интеллектуальной собственности (в т.ч. коммерческой тайны) Компании;

2.7. - обеспечение законных прав юридических лиц и ИП по охране коммерческой тайны;

2.8. - своевременное выявление и устранение угроз объектам информационной безопасности на основе правовых, организационных и инженерно-технических мер и средств обеспечения защиты;

2.9. - обеспечение конституционных прав граждан по сохранению личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах Компании;

2.10. - минимизация ущерба и скорейшее восстановление программных и аппаратных средств, информации, пострадавших в результате кризисных ситуаций, расследование причин возникновения таких ситуаций и принятие соответствующих мер по их предотвращению.

3. СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Организация и функционирование системы информационной безопасности должны соответствовать следующим принципам:

3.1.1. **Обоснованность.** Используемые возможности и средства защиты информационных ресурсов должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности.

3.1.2. **Комплексность.** Предполагает обеспечение защиты информационных ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями, обеспечение согласованности организационных мер и мероприятий, инженерно-технических и программно-аппаратных средств, обеспечение безопасности информационных ресурсов.

3.1.3. **Законность.** Предполагает разработку системы информационной безопасности на основе Федерального законодательства, информатизации и защиты информации и других нормативных актов по безопасности, утвержденных органами государственного управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений.

3.1.4. **Взаимодействие и координация.** Означает осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи Департамента IT, рекламы и маркетинга со всеми Департаментами и Отделами Компании в целях своевременного придания информации конфиденциального статуса, а также оперативного принятия мер в случае

3.1.5. **Совершенствование.** Предусматривает развитие мер и средств обеспечения информационной безопасности на основе собственного опыта, появления новых технических средств.

3.1.6. **Ответственность.** Предусматривает принятие всех законных мер по привлечению к ответственности виновных лиц, вплоть до уголовной, за нарушение порядка обеспечения мер информационной безопасности, предусмотренного действующим законодательством, настоящим Положением и Приказами Директора Компании и Руководителя отдельных организаций.

4. ОБЪЕКТЫ ЗАЩИТЫ

4.1. К объектам информационной безопасности, подлежащим защите, относятся:

- информационные ресурсы с закрытым и ограниченным доступом, составляющие коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, а также акустическая (речевая) информация;

-сведения о пайщиках и их персональных данных, их паевых взносах, поданных ими заявлений и намерениях на приобретение недвижимости, их счетах и банковских картах;

- объекты исключительных прав на интеллектуальную собственность; программы ЭВМ, базы данных, их составляющие части и компоненты. Данные о программах ЭВМ, базах данных и их составляющих частей. Фотографии, рисунки, картины, гравюры, чертежи, схемы и прочие произведения изобразительного искусства. Произведения иного рода, созданные во время или на основе технического задания работодателя (системы управления сайтом, отдельные модули управления, скрипты, плагины и др.). Сценарии; составные произведения (фильмы, сайты).
- сведения об исключительных и авторских правах принадлежащих Компании, а также сведения об использовании их любым способом (включая воспроизведение ; запись в цифровой форме, распространение, импорт, прокат, перевод и иную переработку, практическую реализацию, доведение до всеобщего сведения, включая использование в открытых и закрытых сетях, включение в базы данных и мультимедийную продукцию, регистрацию товарных знаков) и в любой форме на территории Российской Федерации и за ее пределами , об их передаче полностью или частично, в том числе с правом выдачи лицензий любым лицам на условиях, определяемых по усмотрению органов управления ЖНК .
- сведения, ставшие известными сотрудникам в процессе исполнения ими должностных обязанностей;
- средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телефонной, факсимильной, радиосвязи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);
- служебные помещения, в которых хранится и обрабатывается информация закрытого и(или) ограниченного доступа;
- технические средства и системы защиты информационных ресурсов.

5. ОСНОВНЫЕ ВИДЫ УГРОЗ ОБЪЕКТАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1 Определение и прогнозирование возможных угроз и степени их опасности необходимы для обоснования, выбора и реализации защитных мероприятий. Комплексный подход к проблеме защиты информации необходимо проводить с учётом двух факторов: предполагаемой вероятности возникновения угрозы и возможного ущерба от её осуществления. Объективность оценки достигается проведением детального аудита процессов функционирования. Аудит проводится собственными силами или с привлечением сторонних организаций.

5.2 Угрозы можно разделить на внешние и внутренние. При этом последние могут представлять особую опасность. Угрозы объектам информационной безопасности проявляются в виде:

- разглашения конфиденциальной информации;
- утечки конфиденциальной информации через технические средства различного назначения;

- несанкционированного доступа к охраняемым информационным ресурсам;
- несанкционированного уничтожения и модификации информационных ресурсов;
- нарушения работы автоматизированных систем и сетей.

5.3 Источниками угроз могут быть:

- некомпетентность или халатность пользователей или персонала;
- злой умысел, независимо от того, внешним или внутренним относительно систем является источник угрозы;
- умышленное проникновение сторонних лиц в помещения, к аппаратуре и оборудованию;
- случайные события и стихийные бедствия.

6. РАБОТЫ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Работа по обеспечению информационной безопасности включает следующие этапы:

- определение информации, содержащей коммерческую и \или служебную тайну, персональным данным и сроков ее действия;
- категорирование помещений по степени важности обрабатываемой в них информации;
- определение категории информации, обрабатываемой каждой отдельной системой;
- описание системы, определение факторов риска, определение уязвимых мест систем;
- выбор средств и мер защиты для предотвращения воздействия факторов риска и их минимизации;
- выбор средств и мер контроля и управления для своевременной локализации и минимизации воздействия факторов риска.

6.2. Отнесение информации к коммерческой тайне - установление ограничений на распространение информации, требующей защиты. Среди сведений, относимых к категории коммерческой тайны, применительно к Компании можно выделить: деловую информацию о деятельности Компании, финансовую документацию, различные сведения о пайщиках, о клиентах, партнерах, сметы, отчёты, перспективные планы развития, аналитические материалы, исследования и т.п.

Отнесение информации к коммерческой тайне осуществляется в соответствии с принципами законности, обоснованности и своевременности. Обоснованность отнесения информации к коммерческой тайне заключается в установлении путем оценки целесообразности защиты конкретных сведений исходя из жизненно - важных интересов, вероятных финансовых и иных последствий нарушения режима соблюдения коммерческой тайны. Своевременность отнесения сведений к коммерческой тайне заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Чтобы отнесение информации к категории коммерческой тайны приобрело законную силу, оно должно быть оформлено в виде специального «Перечня сведений, составляющих коммерческую тайну Компании (далее Перечень), который разрабатывается и уточняется Юридическим отделом совместно с заинтересованными лицами.

Перечень разрабатывается на основании предложений заинтересованных подразделений с учетом действующего законодательства. В Перечне указываются категории сведений, их степень конфиденциальности, срок действия ограничений на доступ к ним.

Перечень утверждается Директором Компании.

Степень конфиденциальности информации, составляющей коммерческую тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Компании и пайщикам вследствие её распространения.

В соответствии с этим среди информации, относимой к коммерческой тайне, выделяются две: информация закрытого и ограниченного доступа. Информации первого типа присваивается гриф «Коммерческая тайна». Информации второго типа присваивается гриф «ИОД»

Инициатива присвоения грифа «Коммерческая тайна», «ИОД», или его отмена принадлежит Исполнителям или основным пользователям информации, а утверждает гриф - Директор Компании.

6.3. Отнесение информации к служебной тайне - установление ограничений на распространение информации, требующей защиты. Среди сведений, относимых к категории служебной тайны, применительно к Компании можно выделить: деловую информацию о деятельности, финансовую документацию, различные сведения о пайщиках, членах, партнерах, сметы, отчёты, перспективные планы развития, аналитические материалы, исследования, и т.п., кроме тех, которые по Законодательству о ЖНК, некоммерческих организациях и т.п. не подлежат закрытию.

Отнесение информации к служебной тайне осуществляется в соответствии с принципами законности, обоснованности и своевременности. Обоснованность отнесения информации к служебной тайне заключается в установлении путем оценки целесообразности защиты конкретных сведений исходя из жизненно - важных интересов, вероятных вредоносных дезорганизационных, финансовых и иных последствий нарушения режима соблюдения служебной тайны. Своевременность отнесения сведений к служебной тайне заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Чтобы отнесение информации к категории служебной тайны приобрело законную силу, оно должно быть оформлено в виде специального «Перечня сведений, составляющих служебную тайну ЖНК, который разрабатывается и уточняется Юридическим отделом совместно с заинтересованными лицами.

Перечень разрабатывается на основании предложений заинтересованных подразделений с учетом действующего законодательства. В Перечне указываются категории сведений, их степень конфиденциальности, срок действия ограничений на доступ к ним.

Перечень утверждается Директором ЖНК.

Степень конфиденциальности информации, составляющей служебную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Компании вследствие её распространения.

В соответствии с этим среди информации, относимой к служебной тайне, выделяются две: информация закрытого и ограниченного доступа. Информации первого типа присваивается гриф «ДСП». Информации второго типа присваивается гриф «ИОД». Инициатива присвоения грифа «ДСП», «ИОД», или его отмена принадлежит Исполнителям или основным пользователям информации, а утверждает гриф - Директор ЖНК.

6.4. Перечень сведений, составляющих персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, сведения о занимаемой должности и размере заработной платы работника и т.д. В отношении пайщиков ЖНК это дополнительно – размеры пая, счета пайщиков, сведения о их намерениях по приобретению недвижимости. Полученных кредитах и т.п. В Перечне указываются категории сведений, их степень конфиденциальности, срок действия ограничений на доступ к ним.

Перечень утверждается Директором ЖНК.

Степень конфиденциальности информации, составляющей персональные данные, должна соответствовать степени тяжести ущерба, который может быть нанесён безопасности Компании в целом и пайщикам и работнику Компании в частности, вследствие её распространения.

В соответствии с этим среди информации, относимой к персональным данным, выделяются две: информация закрытого и ограниченного доступа. Информации первого типа присваивается гриф «ПД-ДСП». Информации второго типа присваивается гриф «ПД-ИОД». Инициатива присвоения грифа «ПД-ДСП», «ПД-ИОД», или его отмена принадлежит Исполнителям или основным пользователям информации, а утверждает гриф - Директор ЖНК.

7. ПОРЯДОК ДОПУСКА ЛИЦ (сотрудников) К СЛУЖЕБНОЙ ДОКУМЕНТАЦИИ, ИНФОРМАЦИИ И ТЕХНИЧЕСКИМ СРЕДСТВАМ

7.1. Порядок допуска лиц (сотрудников) к служебным документам, техническим средствам и информации, а также мероприятия по обеспечению режима сохранности и конфиденциальности объявляется Приказом Директора Компании под роспись ответственного лица.

7.2. Категории допуска руководящего персонала к работе с документами и информацией:

7.2.1 Директор Компании – допущен в полном объеме.

7.2.2. Финансовый директор – допущен в полном объеме к документам финансово-экономической деятельности Компании.

7.2.3. Главный бухгалтер – допущен в полном объеме к бухгалтерской документации, банковским и налоговым документам.

7.2.4. Секретарь-делопроизводитель допущен к работе с документами, поступающими на регистрацию, на подпись, а также к личным документам сотрудников по кадровому учету.

7.2.5. Руководитель службы персонала - допущен к работе с документацией и информацией, связанной с подбором персонала, учетом и анализом кадровой работы и политики, развития персонала Компании.

7.2.6. Руководитель юридического департамента - допущен в полном объеме ко всем видам документов, касающихся юридического сопровождения деятельности Компании.

7.2.7. Руководитель юридического отдела - допущен к конкретной документации, имеющей характер юридического обоснования деятельности Компании.

7.2.8. Руководитель коммерческого департамента – допущен к работе с информацией и документацией, связанной с коммерческой деятельностью Компании.

7.2.9 Руководитель строительного департамента – допущен к работе с документацией и информацией, связанной со строительной деятельностью компании.

7.2.10. Руководитель департамента безопасности – допущен к работе с документацией и информацией, связанной с деятельностью подразделений, входящих в Компанию.

7.2.11. Руководитель департамента IT, маркетинга и рекламы – допущен к работе с документацией и информацией, связанной с администрированием Интернет-ресурсов и функционированием технических средств, обеспечивающих деятельность Компании.

7.2.12. Секретарь - допущен к работе с документацией и информацией, связанной с регистрацией и учетом документации, проходящей через учет.

7.2.13. Системный администратор – допущен к работе, связанной с техническим обслуживанием всей имеющейся аппаратуры офиса и технической документацией по ней, а также программным обеспечением.

7.2.14. Программист - допущен к работе, связанной с созданием и использованием информационных систем, объектов интеллектуальной собственности компании (сайты, презентации, фильмы, программы ЭВМ, базы данных, как в виде сложных произведений, так и их отдельных частей).

7.2.15. Дизайнер - допущен к работе, связанной с созданием и использованием объектов интеллектуальной собственности компании (сайты, презентации, фильмы, программы ЭВМ, базы данных, изображения, наброски, гравюры, как в виде сложных произведений, так и их отдельных частей).

7.2.16. Копирайтер - допущен к работе, связанной с созданием и использованием объектов интеллектуальной собственности компании (сайты, презентации, фильмы, программы ЭВМ, базы данных, текстов, сценариев, статей как в виде сложных произведений, так и их отдельных частей).

7.2.17. Руководитель Службы безопасности – допущен к любой документации и информации, связанной с безопасностью работы Компании.

7.2.18. Руководители отдельных подразделений, входящих в Компанию – допущены к любой документации и информации, связанной с данным подразделением.

7.3. Руководители структурных подразделений обязаны разработать перечень сведений и технических устройств, к которым допущен подчиненный сотрудник – исполнитель в части касающейся, и передать Директору Компании для оформления их допуска Приказом по Компании.

7.4. Посторонние лица (посетители и клиенты) допускаются к информации и документам в объеме, представляющем ответ на конкретный вопрос в части касающейся.

8. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ РЕЖИМА СОХРАННОСТИ И КОНФИДЕНЦИАЛЬНОСТИ

8.1. Учёт документов в бумажном и электронном виде осуществляется в соответствии с Положением о делопроизводстве и документообороте, а также Положением о договорной работе.

8.2. Перечень Дел, хранящихся и используемых в подразделениях, объявляется Приказом Директора Компании ежегодно по состоянию на 01 января.

8.3. Дела систематизируются и учитываются, хранятся в подразделениях. Ответственные – Руководители подразделений. Вынос Дел из офиса допускается с разрешения Руководителя подразделения.

8.4. Законченные Дела готовятся к архивированию, передаются в Архив установленным порядком.

8.5. Запрещается копирование электронных документов, баз данных и т.п., иначе, чем в целях служебного использования, в соответствии с настоящим Положением, с письменного разрешения руководителя. За несанкционированное копирование

работник подлежит дисциплинарной ответственности вплоть до увольнения, в соответствии с нормами Трудового Кодекса РФ. В случае причинения значительного ущерба работник должен быть привлечен к уголовной, административной и имущественной ответственности в соответствии с действующим законодательством.

8.6. Запрещается выдача справок, выписок, копий документов, как в бумажном, так и в электронном виде без разрешения Руководителя. Выдача справок, сведений, выписок, копий документов и информации по запросу третьих лиц, включая представителей государственных и контролирующих органов, осуществляется только по официальному запросу, с разрешения Директора Компании.

8.7. Запрещается внесение изменений, размещение информации на сайте Компании и сотрудничающих с ней организаций, без письменного разрешения Директора Компании.

8.8. Запрещается внесение несанкционированных изменений в учредительные и корпоративные Положения и документы, Реестры, Базы данных, размещенные на сайтах Компании и входящих в нее организаций, без письменного разрешения Директора Компании.

8.9. Информация, составляющая коммерческую тайну, может передаваться в рамках производственного процесса только в соответствии с Положением об информационной безопасности, Положением о документообороте и деловой переписки, по служебным каналам связи.

8.10. Категорически запрещается использовать личную электронную почту, личные мобильные телефоны и другие средства и каналы коммуникации и копирования, производства аудио- и видеозаписи, не принадлежащие компании, для передачи и размножения служебной информации.

8.11. Технические средства (далее - ТС) и программные продукты, используемые в Компании, учитываются в бухгалтерии согласно Правилам бухгалтерского учета в отношении материальных и нематериальных активов и закрепляются Приказом за ответственными лицами под роспись.

8.12. Проверка наличия, сохранности и состояния технических средств осуществляется в ходе ревизии, проводимой не реже одного раза в год. Ответственность несут руководители подразделений и непосредственно закрепленные за ТС лица.

8.13. Ответственность за техническое состояние, работоспособность и обслуживание, контроль наличия ТС, проведение технических мероприятий по компьютерной безопасности возлагается на Руководителя департамента IT, маркетинга и рекламы.

8.14. Материальную ответственность за наличие и использование по назначению ТС несут непосредственно закрепленные за ТС лица.

8.15. При увольнении, временном отсутствии на срок более 10 суток, убытии в командировку, отпуск и т.п. работники должны передавать документы, Дела и ТС по передаточному акту.

8.16. Ответственный Исполнитель обязан оценить степень конфиденциальности подготовленной или полученной им информации и дать предложения по определению грифа документа своему непосредственному руководителю.

8.17. Ответственность и контроль за обеспечением режима сохранности и конфиденциальности документов, ТС и информации в подразделении возлагается на Руководителя соответствующего подразделения.

8.18. Контроль за обеспечением режима сохранности и конфиденциальности документов, ТС и информации в Компании возлагается на Руководителя Юридического департамента и Руководителя службы безопасности Компании.

9. ПОРЯДОК ДОПУСКА СОТРУДНИКОВ К ИНФОРМАЦИИ, ТЕХНИЧЕСКИМ СРЕДСТВАМ И ПОМЕЩЕНИЯМ

9.1. Категорирование помещений по степени важности хранящейся и обрабатываемой в них информации производится Приказом Директора Компании.

9.2. Порядок допуска в помещения офиса, и лиц, ответственных за них, определяется с учетом п.9.1 настоящего Положения Приказом Директора Компании.

9.3. Порядок допуска сотрудников к конфиденциальной информации определяется настоящим Положением и доводится до их сведения Приказом Директора Компании под роспись в Журнале ознакомления.

9.4. При заключении Трудового договора с сотрудниками, поступающими на работу, руководитель Службы персонала и ответственное за кадровую работу лицо обязаны:

9.4.1. ознакомить сотрудника с Перечнем сведений, составляющих коммерческую тайну Компании под роспись;

9.4.2. ознакомить сотрудника с Перечнем сведений, составляющих служебную тайну Компании под роспись;

9.4.3. ознакомить сотрудника с Перечнем сведений, составляющих персональные данные работников Компании под роспись;

9.4.4. ознакомить сотрудника с настоящим Положением об информационной безопасности Компании под роспись, особое внимание - разделу Ответственности за нарушение требований указанного Положения;

9.4.5. включить в текст Трудового договора ссылку на указанные Положение и Перечни с обязательством работника соблюдения их требований;

9.4.6. заключить с работником Соглашение – Обязательство об ознакомлении с указанными в.п.9.4.1.- 9.4.4. документами и обязательстве их неукоснительно соблюдать, а также об ознакомлении и знании норм об ответственности в случае нарушения.

9.5. Установить ответственных лиц за отдельные помещения офиса:

- Кабинеты 476, 477 - Директор ЖНК;
- Кабинет 470 - гл. бухгалтер,
- Кабинеты 471, - секретарь-делопроизводитель,
- Кабинет 475, 461 - руководитель коммерческого департамента,
- Кабинет 458 - руководитель СРО,
- Кабинет, 462, 465 - системный администратор, руководитель департамента IT
- Кабинет 452 - руководитель службы персонала,
- Кабинет 459 - руководитель юридического департамента, руководитель юридического отдела
- Кабинет 463, 464 - руководитель Службы безопасности.

9.6. Перечень лиц, допущенных к вскрытию (снятию с охраны и постановке на охрану) дверей офиса:

- Директор Компании
- Исполнительный директор Компании.
- Директор по правовым вопросам Компании.
- Начальник Службы безопасности Компании.
- Секретарь-делопроизводитель Компании.
- Руководитель юридического отдела Компании.
- Руководитель финансового департамента Компании.

9.7. Лица, допущенные к вскрытию отдельных помещений офиса – объявляются Приказом Директора Компании.

10. ПОРЯДОК ПРИЕМА ПОСЕТИТЕЛЕЙ ГЛАВНОГО ОФИСА

10.1. Встречает посетителей секретарь, проверяет личность пришедшего и цель прибытия, фиксирует в журнале учета посетителей (приложение №3), по телефонной связи вызывает сотрудника отдела, в которой пришел посетитель.
10.2. Перемещения посетителей по офису производится только в сопровождении сотрудников офиса.
10.3. Нахождение посторонних работников в офисе согласовывается предварительно с руководством Компании и подается утвержденным списком на пост охраны Бизнес-центра.

11. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ и\или СЛУЖЕБНУЮ ТАЙНУ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ , И УТРАТУ ДОКУМЕНТОВ, ИЗДЕЛИЙ И МАГНИТНЫХ НОСИТЕЛЕЙ , СОДЕРЖАЩИХ ТАКИЕ СВЕДЕНИЯ

11.1. Ответственность за разглашение сведений, составляющих коммерческую и\или служебную тайну, персональные данные, и утрату документов, изделий и магнитных носителей, содержащих такие сведения, устанавливается в соответствии с действующим законодательством Российской Федерации.
11.2. Ответственность за разглашение и утрату сведений, содержащих коммерческую и\или служебную тайну, персональные данные, несет персонально каждый сотрудник, имеющий доступ к ним.
11.3. Согласно ч.1 ст.81 п.6 пп. в) Трудового кодекса Российской Федерации расторжение трудового договора по инициативе работодателя с работником (увольнение) возможно в случае:

в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника; (в ред. Федерального закона от 30.06.2006 N 90-ФЗ).

11.4. **Уголовная ответственность работника, имеющего доступ к сведениям составляющим коммерческую тайну.** Статья 183 УК РФ. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну:

1. Собирание сведений, составляющих коммерческую, налоговую или "банковскую" тайну, путём похищения документов, подкупа или угроз, а равно иным незаконным способом -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осуждённого за период до одного года, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, -

наказываются штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осуждённого за период до двух лет с лишением права занимать определенные должности или заниматься определённой деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до трех лет, либо лишением свободы на тот же срок.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

наказываются штрафом в размере до одного миллиона пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, -

наказываются принудительными работами на срок до пяти лет либо лишением свободы на срок до семи лет.

11.5. Дисциплинарная ответственность работника, имеющего доступ к персональным данным других работников и пайщиков

Персональные данные относятся к сведениям, которые охраняются федеральным законом. Неправомерное разглашение персональных данных лицом, в чьи обязанности входит соблюдение правил хранения, обработки и использования такой информации, также является основанием для привлечения этого лица к дисциплинарной ответственности (ст. 90 ТК РФ). Согласно пп. "в" п. 6 ч. 1 ст. 81 ТК РФ трудовой договор с работником может быть расторгнут по причине разглашения охраняемой законом тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе по причине разглашения персональных данных другого работника. Поскольку такое увольнение относится к увольнениям за нарушение трудовой дисциплины, то работника, разгласившего персональные данные, необходимо уволить с соблюдением процедуры, предусмотренной ст. 193 ТК РФ.

11.6. Уголовная ответственность работника, имеющего доступ к персональным данным других работников и пайщиков

В соответствии со ст. 137 УК РФ незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации наказываются штрафом в сумме до 200 тыс. руб. или в размере заработной платы либо иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев.

Часть 2 указанной статьи предусматривает, что те же деяния, совершенные лицом с использованием своего служебного положения, наказываются штрафом в сумме от 100 тыс. до 300 тыс. руб. или в размере заработной платы либо иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев.

Следовательно, если работник, ответственный за хранение, обработку и использование персональных данных других работников, злоупотреблял своими служебными полномочиями, распространял сведения о частной жизни других работников без их согласия, то он может быть привлечен к уголовной ответственности.

11.7. Материальная ответственность работника, имеющего доступ к персональным данным других работников

Статьей 90 ТК РФ предусмотрена материальная ответственность за виновное нарушение норм, регулирующих получение, обработку и защиту персональных данных работников и пайщиков. Так, в результате незаконного распространения информации о персональных данных работника или пайщика последнему может быть причинен моральный вред, подлежащий возмещению работодателем. **В соответствии со ст. 238 ТК РФ работник обязан возместить работодателю причиненный последнему прямой действительный ущерб.** Согласно ч. 2 указанной статьи под прямым действительным ущербом также понимается необходимость возмещения ущерба третьим лицам. Следовательно, если вред работнику был допущен по вине лица, которое было ответственно за неразглашение персональных данных, то работодатель может привлечь последнее к материальной ответственности за ущерб, который был нанесен работнику такими действиями. В соответствии с п. 7 ч. 1 ст. 243 ТК РФ материальная ответственность в полном размере причиненного ущерба возлагается на работника в случае разглашения сведений, составляющих охраняемую законом тайну.

11.8. Гражданско-правовая ответственность работника, имеющего доступ к персональным данным других работников и другой информации ограниченного доступа

В соответствии со ст. 151 ГК РФ, если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в иных случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда. Согласно ч. 2 ст. 1099 ГК РФ моральный вред, причиненный действиями (бездействием), нарушающими имущественные права гражданина, подлежит компенсации в случаях, предусмотренных законом. На основании ст. 152 ГК РФ гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности.

Следовательно, если в результате нарушения норм, регулирующих хранение, обработку и использование персональных данных работника, допущенного лицом, ответственным за осуществление вышеперечисленных действий с персональными данными, работнику причинен имущественный ущерб или моральный вред, то он подлежит возмещению в денежной форме в соответствии со статьями Гражданского кодекса РФ.

В случае причинения вреда юридическому лицу, работником которого является нарушитель, компенсация может быть взыскана судебным порядком **в размере действительного ущерба.**

11.9. Административная ответственность работника, имеющего доступ к персональным данным других работников, пайщиков и другой информации ограниченного доступа

В соответствии с п. 1 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон N 152-ФЗ) персональные данные - любая информация,

относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Согласно ст. 24 Закона N 152-ФЗ лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Аналогичные положения содержатся в ст. 90 ТК РФ.

Статьей 13.11 Кодекса РФ об административных правонарушениях предусмотрена ответственность лиц за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) в виде предупреждения или наложения административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей.

Кроме того, анализ ст. ст. 2, 3, 5, 6 Закона N 152-ФЗ позволяет сделать вывод о том, что персональные данные относятся к информации, доступ к которой ограничен.

В связи с этим нарушитель может быть привлечен к административной ответственности по ст. 13.14 КоАП РФ. Данная статья устанавливает ответственность за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных ч. 1 ст. 14.33 КоАП РФ: наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - от четырех тысяч до пяти тысяч рублей.

Отмечаем, что указанная статья применяется только к случаям разглашения информации, доступ к которой ограничен законом о государственной тайне, коммерческой и\или служебной тайне, персональным данным.

12. ПОРЯДОК ПРИВЛЕЧЕНИЯ К ОТВЕТСТВЕННОСТИ ЗА РАЗГЛАШЕНИЕ ОХРАНЯЕМОЙ ЗАКОНОМ ТАЙНЫ ИЛИ РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласно пп. "в" п. 6 ч. 1 ст. 81 ТК РФ, трудовой договор может быть расторгнут при однократном грубом нарушении работником трудовых обязанностей, а именно в случае разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника.

Отношения, связанные с защитой государственной тайны, регулируются Законом РФ от 21.07.1993 N 5485-1 "О государственной тайне", коммерческой - Федеральным законом от 29.07.2004 N 98-ФЗ "О коммерческой тайне". Каждый из этих актов предусматривает уголовную, административную, гражданско-правовую или дисциплинарную ответственность.

В соответствии со ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" персональными данными является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и т.д.

Исходя из этого определения, сведения о занимаемой должности и размере заработной платы работника являются персональными данными работника. Сведения о персональных

данных пайщика, его намерений по приобретению недвижимости, банковских счетах, размерах пая и членах его семьи, т.п. также являются персональными данными гражданина-пайщика.

В соответствии с п. 7 ст. 86 Трудового кодекса РФ защита персональных данных производится за счет работодателя. Дисциплинарные взыскания предусмотрены ТК РФ. Одним из видов дисциплинарных взысканий является увольнение работника.

В соответствии с п. 43 Постановления Пленума Верховного Суда РФ от 17.03.2004 N 2 "О применении судами Российской Федерации Трудового кодекса Российской Федерации" в случае оспаривания работником увольнения по пп. "в" п. 6 ч. 1 ст. 81 ТК РФ работодатель обязан представить доказательства, свидетельствующие о том, что работник обязывался не разглашать такие сведения.

Согласно п. 8 ст. 86 ТК РФ работники должны быть ознакомлены под роспись с локальным нормативным актом работодателя, устанавливающим порядок хранения и использования персональных данных. Таким актом обычно является положение о персональных данных работников.

Кроме того, доступ к персональным данным в связи с исполнением трудовых обязанностей следует закрепить в должностной инструкции соответствующего работника, взяв при этом с него обязательство об их неразглашении.

При применении дисциплинарного взыскания в виде увольнения работодатель должен иметь документальное подтверждение вины работника, так как на основании ст. 192 ТК РФ дисциплинарное взыскание может быть применено к работнику только в случае неисполнения или ненадлежащего исполнения по его вине трудовых обязанностей.

Пленум Верховного Суда РФ в Постановлении от 17.03.2004 N 2 в п. 53 также указывает на необходимость представления таких доказательств.

Унифицированного документа, подтверждающего факт разглашения персональных данных, не существует. При установлении факта разглашения охраняемой законом тайны необходимо зафиксировать данный факт. Таким документом может служить докладная записка. Она составляется лицом, выявившим указанный факт.

Далее в организации назначается проверка выявленного факта. Для этого создается соответствующая комиссия, которая исследует все обстоятельства, послужившие разглашению тайны. В процессе расследования, руководствуясь ст. 193 ТК РФ, с работника нужно затребовать письменное объяснение. При этом, если по истечении двух рабочих дней указанное объяснение работником не представлено, составляется соответствующий акт. Непредставление работником объяснения не является препятствием для применения дисциплинарного взыскания (ст. 193 ТК РФ).

По результатам работы комиссии составляется акт, в котором отражаются причины совершения дисциплинарного проступка, степень виновности лица, размер причиненного ущерба. Также в акте комиссии должны быть представлены рекомендуемые меры дисциплинарного взыскания к указанному лицу. При этом согласно ч. 5 ст. 192 ТК РФ должны учитываться тяжесть проступка и обстоятельства, при которых он был совершен.

Поскольку увольнение за разглашение персональных данных или сведений, составляющих коммерческую и \или служебную тайну, является увольнением за нарушение трудовой дисциплины, такое увольнение должно быть произведено в порядке, предусмотренном ст. 193 ТК РФ.

Если принято решение расторгнуть трудовые отношения с работником, то оформляется соответствующий приказ (распоряжение). Такой Приказ должен быть издан не позднее одного месяца с момента обнаружения правонарушения.

Как определено ст. 193 ТК РФ, приказ (распоряжение) работодателя о применении дисциплинарного взыскания объявляется работнику под роспись в течение трех рабочих дней со дня его издания, не считая времени отсутствия работника на работе. Если работник отказывается ознакомиться с указанным приказом (распоряжением) под роспись, то составляется соответствующий акт.

Дисциплинарное взыскание может быть обжаловано работником в государственную инспекцию труда и (или) органы по рассмотрению индивидуальных трудовых споров.

Несоблюдение установленных законом требований может повлечь признание наложенного дисциплинарного взыскания недействительным.