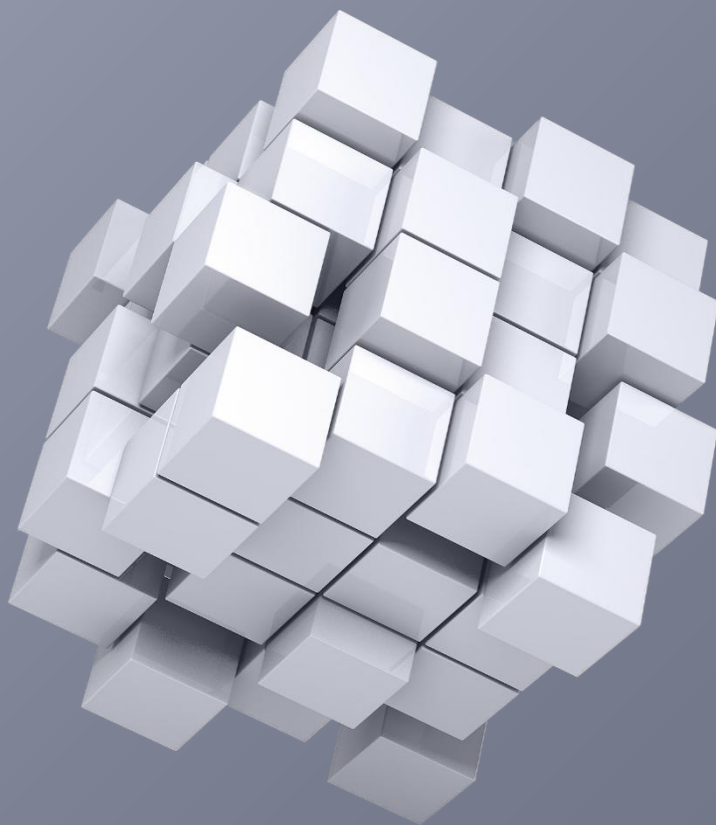




ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «СОФТЛАЙН»

Кодекс поведения и деловой этики



2026 г.

Обращение Владимира Лаврова

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Назначение и ценность Кодекса
- 1.2. Обязательность соблюдения и персональная ответственность
- 1.3. Принятие решений в неопределенных ситуациях

2. О ГРУППЕ КОМПАНИЙ «СОФТЛАЙН»: МИССИЯ И СТРАТЕГИЧЕСКИЕ ИМПЕРАТИВЫ

- 2.1. Миссия и организационная стратегия
- 2.2. Стратегические императивы

3. ПРИНЦИПЫ ДЕЛОВОЙ ЭТИКИ

4. КОРПОРАТИВНЫЕ ЦЕННОСТИ: УПРАВЛЕНЧЕСКИЕ СТАНДАРТЫ КАК ПРАКТИЧЕСКИЕ ОРИЕНТИРЫ ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ

5. РАБОЧАЯ СРЕДА И КУЛЬТУРА ВЗАИМОДЕЙСТВИЯ

- 5.1. Равные возможности и инклюзивность
- 5.2. Психологическая безопасность и культура уважительного взаимодействия
- 5.3. Охрана труда, эргономика и стандарты гибридной работы

6. СОБЛЮДЕНИЕ ЗАКОНОДАТЕЛЬСТВА

- 6.1. Противодействие коррупции
- 6.2. Определение материальных и иных ценностей в контексте антикоррупционных стандартов

7. КОНФЛИКТ ИНТЕРЕСОВ

- 7.1. Определение и область применения
- 7.2. Внешняя занятость и предпринимательская деятельность

8. КОНКУРЕНТНОЕ ПРАВО И РЫНОЧНЫЕ ПРАКТИКИ

- 8.1. Запрет на ограничивающие конкуренцию соглашения
- 8.2. Недопущение практик недобросовестной конкуренции
- 8.3. Исключение конфликта интересов
- 8.4. Обязанность сообщать о нарушениях

9. ОЦЕНКА БЛАГОНАДЕЖНОСТИ КОНТРАГЕНТОВ

- 9.1. Многоуровневая процедура оценки
- 9.2. Комплексная проверка контрагентов

10. ТОРГОВЫЕ ОГРАНИЧЕНИЯ, САНКЦИИ И ЭКСПОРТНЫЙ КОНТРОЛЬ

11. ТОЧНОСТЬ ДЕЛОВЫХ ЗАПИСЕЙ, ФИНАНСОВОЙ И НЕФИНАНСОВОЙ ОТЧЕТНОСТИ

- 11.1. Требования к документальному оформлению и учету
- 11.2. Внутренний контроль и предотвращение искажений
- 11.3. Защита сотрудников и информирование о нарушениях

12. ЗАЩИТА ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ

12.1. Определение и область применения

12.2. Процедуры контроля

13. ПУБЛИЧНЫЕ КОММУНИКАЦИИ, СОЦИАЛЬНЫЕ СЕТИ И ВЗАИМОДЕЙСТВИЕ СО СМИ

14. ЗАЩИТА ИНФОРМАЦИИ, ПЕРСОНАЛЬНЫХ ДАННЫХ И КОММЕРЧЕСКОЙ ТАЙНЫ

14.1. Защита персональных данных

14.2. Защита конфиденциальной информации и коммерческой тайны

15. ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ, КИБЕРБЕЗОПАСНОСТЬ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

15.1. Принципы допустимого использования

15.2. Контроль доступа и защита учетных данных

15.3. Лицензионная дисциплина и управление программным обеспечением

15.4. Ответственность

16. ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ И ОТКРЫТЫЙ ИСХОДНЫЙ КОД

17. ОТВЕТСТВЕННОЕ ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И НОВЫХ ТЕХНОЛОГИЙ

18. ЭКОЛОГИЧЕСКАЯ И СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ

19. СООБЩЕНИЕ О НАРУШЕНИЯХ, РАССЛЕДОВАНИЯ И ЗАЩИТА ОТ ПРЕСЛЕДОВАНИЯ

19.1. Ответственность за нарушения

19.2. Подтверждение ознакомления и обучение сотрудников

19.3 Пересмотр документа

Обращение Владимира Лаврова

Дорогие коллеги,

Когда я думаю о том, что является сильной стороной нашей компании, первое, что приходит в голову, — это не строчки кода, не продуктовые релизы и не финансовые отчеты. Это люди. Именно ваш ежедневный выбор, честность и готовность ставить этические принципы выше сиюминутной выгоды формируют ДНК Группы компаний «Софтлайн».

Кодекс поведения и деловой этики — не формальный документ и не свод запретов. Это наш общий договор о том, как мы хотим работать, принимать сложные решения и влиять на мир вокруг нас. Технологии меняются стремительно, но фундамент остается неизменным: доверие клиентов, уважение к каждому сотруднику, прозрачность и ответственность за последствия наших решений. Особенно сегодня, когда алгоритмы и данные затрагивают жизнь миллионов.

Как руководитель Группы я хочу быть предельно честным: мы не требуем от вас безупречности, но требуем осознанности. Если вы видите нарушение, сомневаетесь в этичности задачи или чувствуете давление — говорите об этом. Мы выстроили и будем развивать механизмы, в которых ваше слово будет услышано, а вы — защищены от любых форм преследования.

Руководители несут особую ответственность за культуру открытого диалога в командах. Они обязаны не допускать любое давление на сотрудников, которые задают вопросы или сообщают о рисках. Я лично убежден: устойчивая культура строится на доверии и взаимной ответственности.

Этот документ будет дополняться и меняться вместе с нами. Но его главный принцип останется неизменным: **мы создаем технологии для людей, сохраняя человечность и этическую чуткость.**

Спасибо за то, что вы часть нашей Группы. Берегите нашу репутацию, задавайте неудобные вопросы и помните: каждый ваш выбор формирует наше общее будущее.

С уважением и верой в наше общее дело,

Владимир Лавров



ОБЩИЕ ПОЛОЖЕНИЯ

Назначение и ценность Кодекса

Независимо от внешних изменений, Группа компаний «Софтлайн» (далее — «Софтлайн», Компания, Группа) сохраняет приверженность высшим стандартам деловой этики. Наша репутация — ключевой нематериальный актив, требующий системной защиты и управления. Кодекс поведения и деловой этики (далее — Кодекс) фиксирует этические обязательства Компании, основанные на принципах добросовестности, справедливости и законности, и определяет стандарты поведения в ситуациях, способных повлиять на деловую репутацию Группы.

Документ опирается на российское законодательство и международные нормы делового поведения. Он отражает стремление «Софтлайна» работать в соответствии с этическими принципами и уважать права человека. Требования Кодекса обязательны **для всех сотрудников — независимо от их должности и уровня ответственности, формата занятости и региона.**

Высокие стандарты взаимодействия — основа долгосрочного доверия акционеров, клиентов, поставщиков и профессионального сообщества.

Обязательность соблюдения и персональная ответственность

Каждый член команды «Софтлайна» обязан соблюдать Кодекс. Акционеры, члены Совета директоров и топ-менеджеры должны быть этическими лидерами и достойно представлять Группу публичной среде.

Нарушение положений Кодекса влечет применение мер дисциплинарного воздействия вплоть до расторжения трудового договора. Отдельные нормы Кодекса дублируют требования законодательства, поэтому недобросовестные действия могут повлечь гражданско-правовую, административную или уголовную ответственность.

Каждый сотрудник действует от имени Группы: неэтичное поведение любого из нас создает репутационные, финансовые и правовые риски для всей Компании.

Кодекс имеет приоритет над другими внутренними документами и служит основой для разработки политик, процедур и регламентов «Софтлайна».

Ключевые обязательства

- Следовать принципам Кодекса в любых обстоятельствах.
- Соблюдать внутренние политики, регламенты и применимое законодательство.
- При отсутствии прямых указаний в Кодексе или законе обращаться за разъяснениями в юридическое управление или управление персоналом и руководствоваться принципами этики и здравым смыслом.
- Немедленно сообщать об известных или предполагаемых нарушениях через защищенные каналы информирования.

Принятие решений в неопределенных ситуациях

Кодекс не может охватить все возможные ситуации, так как бизнес-среда постоянно меняется. Его задача — дать сотрудникам ценностный компас для принятия взвешенных решений.

Если ситуация не описана в Кодексе или вызывает сомнения, следует оценить свои действия по следующим критериям.

Законность. Соответствует ли мой поступок нормам применимого законодательства?

Этичность. Согласуется ли он с ценностями «Софтлайна» и общепринятыми моральными нормами?

Публичность. Готов ли я открыто сообщить о нем коллегам, руководству или близким?

Репутационный риск. Не нанесет ли это ущерб деловой репутации Компании?

Влияние на людей и данные. Не нарушит ли это чьи-то права, безопасность, приватность, финансовые интересы или доверие людей? Не пострадают ли персональные и клиентские данные?

Если хотя бы на один вопрос вы ответили отрицательно, то следует отказаться от планируемого действия.

Важно!

В ситуациях, не имеющих однозначного регулирования, руководствуйтесь **принципами честности, справедливости и недопущения вреда**. Если сомневаетесь, как поступить, проконсультируйтесь с руководителем или представителями юридического департамента и управления персоналом.

О ГРУППЕ КОМПАНИЙ «СОФТЛАЙН»: МИССИЯ И СТРАТЕГИЧЕСКИЕ ИМПЕРАТИВЫ

Миссия и организационная стратегия

В 2025 году «Софтлайн» завершил трансформацию в инвестиционно-технологический холдинг, перейдя от точечного внедрения инструментов к созданию устойчивой цифровой архитектуры. Основой операционной модели стал кластерный принцип, который обеспечивает глубину экспертизы и ответственность за результат в ключевых направлениях. Группа объявила о создании трех кластеров:

FabricaONE.AI — лидирующий разработчик программного обеспечения на основе ИИ.

«СФ Тех» — разработка и внедрение высокотехнологичных решений для корпоративных, промышленных и инфраструктурных заказчиков.

«Цифровые Решения» — лидирующий ИТ-поставщик продуктов и услуг для цифровой трансформации и в области информационной безопасности.

Такая структура позволяет формировать для клиентов комплексные экосистемные предложения с измеримым бизнес-эффектом, которые применимы и в отраслях с высокими требованиями к надежности: промышленности, энергетике и государственном секторе. При этом обеспечивается прозрачность и предсказуемость для инвесторов и партнеров.

Стратегические императивы

Стратегия Компании реализуется через четыре взаимосвязанных принципа управления:

Фокус на продуктах с высокой добавленной стоимостью. Мы последовательно увеличиваем долю собственных высокомаржинальных решений в портфеле, что является основным драйвером роста рентабельности и фундаментом устойчивости бизнеса.

Синергия кластеров и кросс-функциональное взаимодействие. Кластеры работают как единая экосистема — обмениваются экспертизой, клиентскими инсайтами и каналами дистрибуции. Такой подход является стандартом работы, который исключает дублирование функций и внутренние барьеры.

Финансовая дисциплина и управление рисками. Политика управления капиталом и долгом синхронизирована с операционными денежными потоками. Это обеспечивает финансовую устойчивость Компании в условиях рыночной волатильности и соблюдение интересов всех заинтересованных сторон.

Человеческий капитал в парадигме AI First. Повышаем производительность за счет системной автоматизации и внедрения искусственного интеллекта (ИИ) во внутренние процессы. Мы используем ИИ как этический инструмент для усиления потенциала сотрудников, а не для их замещения.

ПРИНЦИПЫ ДЕЛОВОЙ ЭТИКИ

Настоящий раздел определяет обязательные стандарты поведения для каждого сотрудника и партнера компании. Наши принципы — основа для принятия решений, оценки действий и формирования долгосрочного доверия, а не просто рекомендации.

Добросовестность и ответственность

Мы действуем честно и открыто как внутри компании, так и за ее пределами. «Софтлайн» гарантирует исполнение взятых обязательств в установленные сроки и в соответствии с высшими стандартами деловой практики. Группа исключает любые формы сокрытия информации, манипуляций или предоставления противоречивых сведений. Как ответственный работодатель, «Софтлайн» обеспечивает прозрачные, измеримые и справедливые механизмы мотивации, оценки и вознаграждения.

Справедливость и равные возможности

Мы принимаем все решения исключительно на основе объективных фактов, профессиональных критериев и установленных процедур, без влияния личных предпочтений, предрассудков или конфликта интересов. «Софтлайн» гарантирует равные возможности для профессионального роста, развития и реализации потенциала каждого сотрудника, а также строит отношения с партнерами на принципах уважения и равенства. Справедливость — неотъемлемая часть нашей корпоративной культуры и деловой репутации.

Социальная ответственность

«Софтлайн» осознает масштаб влияния технологий на общество и берет на себя ответственность за социальные, экологические и экономические последствия своей деятельности. Мы разрабатываем и внедряем цифровые продукты, направленные на устойчивое развитие, повышение качества жизни и поддержку общественных благ. Каждое стратегическое и операционное решение оценивается через призму долгосрочного позитивного влияния на клиентов, партнеров, общество и будущие поколения. Мы не допускаем действий, которые могут нанести прямой или косвенный ущерб интересам третьих лиц.

Законность

Деятельность «Софтлайна» строится на строгом соблюдении российского и применимого международного законодательства, отраслевых стандартов и внутренних процедур. Компания отвергает любые попытки достижения бизнес-целей незаконными, неэтичными или коррупционными методами. Мы развиваем эффективные системы внутреннего контроля, оперативно выявляем, расследуем и пресекаем нарушения, а также непрерывно совершенствуем процессы, чтобы свести к минимуму правовые и репутационные риски.

Этическая культура

Этика — стратегический приоритет и основа устойчивого развития «Софтлайна». Мы создаем среду, в которой каждый руководитель подает личный пример и принимает взвешенные решения в сложных ситуациях. Адаптация новых сотрудников к этическим ценностям компании, регулярное обучение и аттестация по стандартам делового поведения — обязательные элементы корпоративной стратегии. Каждый сотрудник имеет право и обязан действовать в соответствии с настоящими принципами, а также сообщать о возможных нарушениях без риска преследования.

КОРПОРАТИВНЫЕ ЦЕННОСТИ: УПРАВЛЕНЧЕСКИЕ СТАНДАРТЫ КАК ПРАКТИЧЕСКИЕ ОРИЕНТИРЫ ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ

Описанные в этом разделе ценности определяют стратегические приоритеты «Софтлайна» и служат ориентиром для ежедневных решений, коммуникаций и оценки эффективности. Они дополняют фундаментальные принципы Кодекса, переводя этические нормы в конкретные управленческие и операционные стандарты.

Лидерство с этической ответственностью

Мы задаем отраслевые стандарты и выступаем ответственным партнером для бизнеса, регуляторов и профессионального сообщества. Наша экспертиза направлена не только на коммерческий успех, но и на создание прозрачных, безопасных и устойчивых экосистем. Руководители и эксперты обязаны делиться знаниями, прогнозировать долгосрочные последствия технологических изменений и следить за тем, чтобы лидерство компании не противоречило интересам рынка, общества и этическим нормам.

Ориентация на клиента и прозрачность взаимодействия

Интересы клиента — приоритет нашей деятельности. Мы предлагаем решения, основанные на объективной оценке потребностей, честной коммуникации и долгосрочной ценности. Мы не продвигаем избыточные технологии, не скрываем риски или не манипулируем информацией в коммерческих интересах. Каждое взаимодействие строится на профессиональной честности, защите данных и приоритете бизнес-результатов клиента над краткосрочной выгодой Компании.

Единая команда: доверие, развитие и культура сопричастности

Мы формируем среду открытого партнерства, в которой сотрудник — соавтор успеха Компании. «Софтлайн» гарантирует равный доступ к профессиональному росту, признает вклад каждого и поощряет инициативы, которые направлены на повышение операционной эффективности и устойчивости бизнеса. Мы развиваем ответственное отношение к общим результатам. Сотрудники осознают, как их решения влияют на Компанию, коллег и конечных пользователей, и соблюдают принципы взаимного уважения, психологической безопасности и коллективной подотчетности.

Ответственные инновации и технологическое развитие

Инновации «Софтлайна» направлены на создание безопасных, масштабируемых и этических технологических решений. Перед внедрением новых технологий Компания оценивает их влияние на пользователей, клиентов, отрасль, экологию, а также на безопасность информационных систем и данных. Технологический прогресс должен сопровождаться этической, правовой и регуляторной оценкой, особенно если решение затрагивает персональные сведения, критическую инфраструктуру, автоматизированное принятие решений и ИИ.

Ответственность

Основа нашей корпоративной культуры — ответственность перед клиентами, сотрудниками, акционерами и обществом. Мы соблюдаем требования законодательства и следуем передовым стандартам корпоративного управления. Это гарантирует прозрачную отчетность, независимый контроль и ответственность руководства. Мы выполняем в полном объеме все стратегические обещания, контрактные обязательства и внутренние стандарты. Нарушение этих принципов Компания рассматривает как системный репутационный и операционный риск и пресекает.

РАБОЧАЯ СРЕДА И КУЛЬТУРА ВЗАИМОДЕЙСТВИЯ

Настоящий раздел определяет обязательные требования к организации рабочего пространства, коммуникационных практик и охраны труда. Стандарты действуют для всех подрядчиков, сотрудников и временного персонала независимо от формата занятости (офис, удаленная или гибридная работа).

Равные возможности и инклюзивность

«Софтлайн» создает инклюзивную рабочую среду, в которой сотрудников оценивают исключительно по их профессиональным компетенциям, измеримым результатам труда и потенциалу развития. Подбор, адаптация, аттестация и карьерный рост строятся на основе объективных критериев. Мы исключаем влияние личных предпочтений, стереотипов или скрытых предубеждений. Компания гарантирует равный доступ к внутренним возможностям, обучению и проектной деятельности независимо от национальности, пола, возраста, вероисповедания, мировоззрения, особенностей здоровья, сексуальной ориентации, политических взглядов, социального происхождения.

Любая дискриминация, предвзятое отношение или искусственные барьеры для профессионального роста категорически запрещены.

Психологическая безопасность и культура уважительного взаимодействия

Группа придерживается политики абсолютной нетерпимости к любым формам домогательств, агрессивного поведения, запугивания, притеснения, дискриминационных высказываний и психологического давления. Все участники корпоративных процессов обязаны поддерживать профессиональный, уважительный и конструктивный тон во всех каналах коммуникации: при личном взаимодействии, в офисных пространствах и цифровой среде (в корпоративных мессенджерах, видеоконференциях, платформах совместной работы, электронной почте, ИИ-ассистентах и чат-ботах).

«Софтлайн» формирует условия психологической безопасности, при которых сотрудники могут открыто выражать профессиональное мнение, задавать вопросы и сообщать о нарушениях без риска негативных последствий.

Руководители несут персональную ответственность за предотвращение неэтичного поведения в своих командах. Они обязаны оперативно реагировать на сигналы о подобных ситуациях и поддерживать здоровую культуру общения.

Охрана труда, эргономика и стандарты гибридной работы

«Софтлайн» обеспечивает безопасные, эргономичные и технологичные условия труда. Компания соблюдает все применимые требования законодательства в области охраны труда, промышленной безопасности и профилактики профессиональных заболеваний. Мы регулярно оцениваем риски, обучаем персонал и оснащаем рабочие места сертифицированным оборудованием.

Компания внедряет стандарты цифровой гигиены, оптимизирует информационную нагрузку и делает все необходимое для профилактики профессионального выгорания.

СОБЛЮДЕНИЕ ЗАКОНОДАТЕЛЬСТВА

Противодействие коррупции

«Софтлайн» придерживается политики абсолютной нетерпимости к коррупции и взяточничеству. Мы исходим из принципа, что коррупционные практики искажают рыночные механизмы и нарушают основы свободной конкуренции.

Запрет на неправомерное влияние

Категорически запрещается предлагать, обещать, передавать или получать материальные и нематериальные выгоды — напрямую или через посредников, в том числе через третьих лиц (агентов, консультантов, подрядчиков, дистрибьюторов и реселлеров), в целях получения коммерческих, административных или регуляторных преимуществ. Стандарт распространяется на взаимодействие с государственными и муниципальными служащими, представителями организаций с государственным участием, а также коммерческими контрагентами. **Передача ценностей супругам, детям или другим близким родственникам должностных лиц юридически приравнивается к передаче самому лицу.**

Регламентация допустимых расходов

Благотворительная деятельность, спонсорство, представительские расходы, участие в конференциях, деловые поездки, подарки и другие формы делового гостеприимства не могут использоваться как инструмент влияния на закупочные, регуляторные, кадровые или иные решения. Такие расходы допускаются только в рамках применимого законодательства и внутренних регламентов, подлежат документальному подтверждению, должны быть соразмерны, прозрачны и преследовать законные деловые цели. Конкретные лимиты, порядок согласования и регистрация устанавливаются отдельными документами.

Подотчетность и ответственность

Настоящие стандарты применяются ко всем сотрудникам, руководителям и партнерам Группы. Любые признаки коррупционных взаимодействий должны обязательно фиксироваться, а информация незамедлительно передаваться в функцию комплаенса. Нарушение норм квалифицируется как грубое дисциплинарное правонарушение и может повлечь гражданско-правовую, административную или уголовную ответственность.

Определение материальных и иных ценностей в контексте антикоррупционных стандартов

Под материальными и иными ценностями понимаются **любые выгоды имущественного и неимущественного характера**, которые могут использоваться для неправомерного влияния. Приведенный в Кодексе перечень не является исчерпывающим и служит примером.

Финансовые выгоды и денежные эквиваленты

- Денежные средства в любой валюте и форме передачи.
- Подарочные карты, сертификаты, ваучеры и другие платежные инструменты.
- Скидки, преференции или особые условия предоставления продуктов и услуг, недоступные широкому кругу покупателей.

Подарки и деловое гостеприимство

- Подарки любой стоимости, включая сувениры, если они существенно превышают стоимость традиционной брендовой продукции.
- Оплата или компенсация расходов на развлечения, культурные и спортивные мероприятия.
- Оплата транспортных расходов, проживания, питания и других затрат, связанных с приемом контрагентов.

Трудоустройство и карьерные преимущества

- Предложения о трудоустройстве, в том числе для родственников, супругов или иных близких лиц государственных должностных лиц и представителей контрагентов.
- Обещания предоставления работы или карьерных перспектив в будущем в обмен на лояльность или принятие решений в пользу «Софтлайна».

Услуги, образование и личные преференции

- Оплата обучения, повышения квалификации, участия в конференциях и профессиональных мероприятиях.
- Предоставление личных услуг (бытовых, консультационных, представительских) на безвозмездной или льготной основе.

Благотворительные и политические взносы

- Пожертвования на благотворительные цели, если они могут быть интерпретированы как инструмент влияния на деловые решения.
- Взносы в поддержку политических партий, кампаний или общественных организаций, связанных с государственными должностными лицами.

Принцип применения

Любая передача ценностей, независимо от формы, номинальной стоимости или канала передачи (напрямую или через третьих лиц), оценивается на предмет соответствия антикоррупционным стандартам. Ключевой критерий — не формальная категория выгоды, а ее потенциальная способность повлиять на независимость принятия решений.

При сомнениях в допустимости передачи ценности сотрудник обязан запросить предварительное согласование в команде комплаенса юридического управления.

КОНФЛИКТ ИНТЕРЕСОВ

«Софтлайн» уважает частную жизнь сотрудников, однако объективность, справедливость и прозрачность корпоративных процессов имеют безусловный приоритет. Личные интересы не должны влиять на профессиональные решения или создавать риски, подрывающие деловую репутацию.

Определение и область применения

Конфликт интересов возникает, когда личная, семейная, финансовая или иная заинтересованность сотрудника (прямая или косвенная) влияет или может быть объективно воспринята как влияющая на выполнение должностных обязанностей, принятие управленческих или коммерческих решений. Стандарт распространяется на взаимодействия с контрагентами, поставщиками, клиентами, конкурентами и другими стейкхолдерами, если личные связи способны исказить условия сотрудничества или оценку результатов.

Критерии значимых связей

К лицам, чьи интересы могут создавать конфликт, относятся близкие родственники: супруг(а), родители, дети, братья/сестры, бабушки/дедушки, внуки, совместно проживающие партнеры. Сюда же относятся люди, с которыми сотрудника связывают тесные дружеские, финансовые или доверительные отношения. При взаимодействии с такими лицами сотрудник обязан самостоятельно оценивать риск утраты объективности и действовать в соответствии с принципами прозрачности.

Ограничения и запреты

Совместная работа близких родственников в Компании возможна, но строго запрещено прямое или функциональное подчинение друг другу. Сотрудники обязаны избегать ситуаций, в которых личные интересы могут повлиять на их профессиональные решения.

Компания придерживается политики нулевой терпимости к протекционизму. Нанимать или переводить родственников допускается только при отсутствии потенциального конфликта и с предварительного согласования директора по персоналу Группы и службы безопасности.

Каждый сотрудник обязан незамедлительно декларировать любой фактический или потенциальный конфликт интересов, включая изменение личных обстоятельств или появление новых связей с контрагентами. Соккрытие конфликта или продолжение деятельности в таких условиях — грубое нарушение Кодекса. Выявленные случаи передаются на оценку юридического управления и управления безопасности для минимизации рисков. Меры могут быть разными: отвод от принятия решений, изменение зоны ответственности, перевод в другое подразделение или иные организационные меры.

Внешняя занятость и предпринимательская деятельность

«Софтлайн» исходит из принципа приоритета корпоративных обязанностей и полной профессиональной вовлеченности сотрудников. Любая внешняя занятость, предпринимательская активность или участие в сторонних бизнес-проектах подлежат обязательному декларированию и не должны создавать конфликта интересов, снижать эффективность вашей работы или наносить ущерб репутации Компании.

Допустимые формы участия в сторонних организациях

Сотрудникам разрешено пассивное инвестирование в капитал других организаций (владение акциями, облигациями, паями), если такое участие не предполагает операционного управления, не создает конфликта интересов и не противоречит антимонопольному законодательству.

Категорически запрещается

- Учреждать, регистрировать или руководить юридическими лицами, чья деятельность совпадает, конкурирует или пересекается с деятельностью «Софтлайна» и компаний Группы.
- Занимать должности в органах управления сторонних организаций, если это требует существенных временных затрат, влияет на объективность принятия решений или создает риски утечки конфиденциальной информации.
- Использовать корпоративные ресурсы, информацию, контакты или репутацию «Софтлайна» в личных предпринимательских целях.

Процедура декларирования

Любая фактическая или планируемая внешняя занятость, участие в капитале или органах управления сторонних организаций должны предварительно письменно декларироваться через установленные каналы юридической функции или HR вашей бизнес-единицы. Если ситуация вызывает сомнения, несет высокие риски или явный конфликт интересов, запрос направляется на согласование на уровень Группы. Скрытие информации или уклонение от декларирования квалифицируется как нарушение Кодекса.

КОНКУРЕНТНОЕ ПРАВО И РЫНОЧНЫЕ ПРАКТИКИ

«Софтлайн» придерживается принципов свободной рыночной конкуренции как основы технологического прогресса и экономического развития. Мы конкурируем исключительно за счет профессиональных компетенций, качества решений и эффективности сервисов и работаем в строгом соответствии с антимонопольным законодательством и внутренними стандартами деловой этики.

Запрет на ограничивающие конкуренцию соглашения

Категорически запрещается вступать в картельные сговоры или координировать действия с конкурентами, включая согласование цен, скидок, маржинальности, условий торгов, клиентов, территорий, а также графиков поставок, тендерных стратегий, условий найма, планов вывода продуктов или ограничения объемов предложения. Компания участвует в тендерных и конкурсных процедурах на общих основаниях, без предварительных договоренностей с заказчиками или другими участниками и без использования конфиденциальной информации для получения необоснованных преимуществ.

Недопущение практик недобросовестной конкуренции

Запрещается использовать незаконные или неэтичные методы конкурентной разведки, распространять ложные или вводящие в заблуждение сведения о конкурентах, а также дискредитировать их деловую репутацию. Компания объективно формирует ценовую политику: не допускает установление монопольно высоких или демпингово низких цен с целью ограничения конкуренции или вытеснения участников рынка.

На конференциях, в отраслевых ассоциациях, рабочих группах и профессиональных сообществах сотрудники обязаны избегать обсуждения коммерчески чувствительной информации, способной ограничить конкуренцию или создать видимость координации действий с конкурентами.

Запрещается использовать алгоритмы, платформы, аналитические инструменты, ИИ-системы или обмен данными для координации цен, раздела рынка, ограничения конкуренции либо получения недобросовестного преимущества.

Исключение конфликта интересов

Компания выбирает поставщиков и партнеров на основе прозрачных, измеримых и объективных критериев. Запрещено нанимать бывших государственных служащих или их близких родственников, если основной мотив — наладить неправомерные контакты или получить преференции от регулирующих органов. Переманивание сотрудников или клиентов конкурентов допускается только рыночными и этичными методами, которые исключают использование служебной тайны, конфликт интересов или недобросовестное влияние.

Обязанность сообщать о нарушениях

О любых фактах или признаках недобросовестной конкуренции, антиконкурентных соглашений или злоупотребления доминирующим положением необходимо незамедлительно сообщить в юридическое управление и управление безопасности. «Софтлайн» гарантирует анонимность и защиту сотрудникам, добросовестно сообщившим о потенциальных нарушениях в рамках настоящей политики.

ОЦЕНКА БЛАГОНАДЕЖНОСТИ КОНТРАГЕНТОВ

«Софтлайн» применяет риск-ориентированный подход к оценке контрагентов до инициирования сотрудничества. Глубина и формат проверки масштабируются пропорционально уровню потенциальных юридических, финансовых и репутационных рисков.

Многоуровневая процедура оценки

Проверка проводится согласованно профильными службами Компании:

- **Юридический блок:** анализ регистрационных данных, судебной истории, сведений о реорганизации или банкротстве, а также мониторинг публикаций в открытых источниках.
- **Финансовый блок:** верификация финансовой отчетности, проверка налоговой дисциплины, оценка платежеспособности и устойчивости бизнес-модели.
- **Блок безопасности:** оценка деловой репутации контрагента и его руководства, проверка наличия исполнительных производств, административных и уголовных дел.

Комплексная проверка контрагентов

Официальное заключение о благонадежности формируется на основе сводных данных. Взаимодействие разрешается исключительно при положительном вердикте. Регулярные процедуры комплексной проверки гарантируют, что контрагенты разделяют этические, правовые и операционные стандарты «Софтлайна». Процедура проверки — обязательное требование Группы.

В зависимости от уровня риска оценка контрагента включает проверку санкционных и торговых ограничений, коррупционных рисков, конфликта интересов, финансовой устойчивости, деловой репутации, соблюдения прав человека и трудовых практик, информационной безопасности, обработки персональных данных, использования ИИ, субподрядчиков, бенефициаров и аффилированности.

Проверка проводится до начала сотрудничества и в ходе отношений с контрагентом при изменении собственников, юрисдикции, характера услуг, доступа к данным, уровня риска или иных существенных обстоятельств.

В договорах с контрагентами мы закрепляем обязательства соблюдать нормы противодействия коррупции и права человека, стандарты конфиденциальности, информационной безопасности и защиты персональных данных, а также следовать Кодексу поставщика и принципам ответственного использования ИИ.

ТОРГОВЫЕ ОГРАНИЧЕНИЯ, САНКЦИИ И ЭКСПОРТНЫЙ КОНТРОЛЬ

«Софтлайн» соблюдает применимые торговые ограничения. Сотрудники обязаны учитывать ограничения по клиентам, конечным пользователям, странам назначения, вендорам, технологиям, лицензиям и способам поставки.

Запрещается участвовать в обходных схемах, использовать посредников для сокрытия конечного пользователя, дробить сделки, искажать описание продукта, услуги или маршрута поставки, а также передавать технологии, данные или программное обеспечение, если есть сомнения в законности такой передачи.

При любом сомнении в допустимости сделки, поставки, доступа к технологии, использования облачного сервиса, передачи исходного кода, документации или оказания технической поддержки сотрудник обязан до совершения действия обратиться в юридическое управление.

ТОЧНОСТЬ ДЕЛОВЫХ ЗАПИСЕЙ, ФИНАНСОВОЙ И НЕФИНАНСОВОЙ ОТЧЕТНОСТИ

«Софтлайн» обеспечивает полноту, точность и достоверность финансовой, управленческой, проектной, операционной, ИБ и иной деловой отчетности. Это основа корпоративного управления и доверия акционеров. Все хозяйственные операции, проектные решения, тендерные материалы, ключевые показатели эффективности, расходы, трудозатраты, инциденты, результаты аудитов и существенные бизнес-события отражаются своевременно, в полном объеме и на основании подтверждающих данных.

Требования к документальному оформлению и учету

Достоверность отчетности начинается с уровня каждого первичного документа и деловой записи: счетов, актов, накладных, платежных поручений, расходных документов, CRM-записей, проектной документации, отчетов по выполнению ключевых показателей эффективности, ИИ-метрик и журналов безопасности. Запрещается регистрировать сделки в обход учетных систем, использовать неофициальные записи, создавать параллельную документацию или изменять данные без законного основания и авторизации.

Внутренний контроль и предотвращение искажений

Система внутреннего контроля предназначена для своевременного выявления и пресечения попыток сокрытия неправомерных платежей, манипуляций с отчетностью, корпоративного мошенничества или искажения деловых записей. Регулярные аудиты и сверки обеспечивают разумную уверенность в соответствии применимым стандартам и законодательству. Сокрытие данных, предоставление ложной информации, уничтожение документов, давление на аудиторов или введение в заблуждение представителей внутреннего контроля рассматриваются как нарушение Кодекса.

Защита сотрудников и информирование о нарушениях

«Софтлайн» гарантирует всестороннюю поддержку и защиту от преследований любому сотруднику, который отказался участвовать в искажении учетных данных или сообщил о выявленных нарушениях через защищенные каналы. Участие в фальсификации отчетности, умышленное сокрытие информации или создание условий для недостоверного учета квалифицируется как грубое дисциплинарное правонарушение и может повлечь гражданско-правовую, административную или уголовную ответственность.

Запрещается

- Искажать, скрывать или избирательно отражать данные, подлежащие обязательному учету.
- Формировать отчетность на основании неофициальных, неподтвержденных или сфальсифицированных документов.
- Оказывать давление на сотрудников бухгалтерии, финансового/внутреннего контроля или внутреннего аудита с целью влияния на учетные решения.

О любых фактах или признаках недостоверного учета необходимо незамедлительно сообщить в функцию комплаенса или внутреннего аудита.

ЗАЩИТА ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ

«Софтлайн», являясь публичной компанией (Московская биржа, тикер: SOFL), соблюдает законодательство в области противодействия неправомерному использованию инсайдерской информации и манипулированию рынком (далее – ПНИИИМР), рекомендации Банка России в области ПНИИИМР. Защита инсайдерской информации с целью предотвращения неправомерного использования указанной информации и манипулирования рынком — фундаментальное обязательство «Софтлайн» перед акционерами, инвесторами и профессиональным сообществом.

Определение и область применения

Инсайдерская информация — это точная и конкретная информация, которая не была распространена, и распространение которой может оказать существенное влияние на рыночную стоимость ценных бумаг «Софтлайна». К такой информации относятся:

- сведения о созыве, проведении заседания общего собрания акционеров, а также о принятых на нем решениях;
- информация о размещении или погашении ценных бумаг и об осуществлении прав по ним;
- выявленные ошибки в ранее раскрытой финансовой отчетности;
- данные годовой и промежуточной финансовой отчетности до момента их официального опубликования;
- сведения о проведении заседания совета директоров общества и его повестке дня, а также о принятых решениях, включая рекомендации по размеру дивидендов по акциям и порядку их выплаты;
- другие сведения, включенные в утвержденный перечень инсайдерской информации компании.

Актуальная версия перечня размещена в открытом доступе на сайте общества:
<https://softlinegroup.com/investors/disclosure-centrer/>.

Категорически запрещается:

- использовать инсайдерскую информацию для совершения сделок с ценными бумагами;
- давать рекомендации или побуждать третьих лиц к совершению сделок с ценными бумагами, если такие рекомендации основаны на инсайдерской информации;
- разглашать инсайдерскую информацию третьим лицам до ее официального раскрытия обществом;
- совершать сделки в «тихие периоды», установленные в соответствии с внутренними документами «Софтлайна»;
- осуществлять действия, приводящие к манипулированию рынком, включая умышленное распространение заведомо ложных сведений, совершение сделок, искусственно влияющих на котировки или объемы торгов;
- обсуждать нераскрытую инсайдерскую информацию в неавторизованных каналах коммуникации, включая личные беседы, мессенджеры, социальные сети и внешние цифровые платформы.

Процедуры контроля

Доступ к инсайдерской информации предоставляется при соблюдении установленного внутренними документами порядка, в связи с исполнением трудовых или гражданско-правовых обязанностей, а также обязанностей, установленных федеральными законами. Сотрудники и другие лица, имеющие доступ к таким сведениям, обязаны:

- соблюдать режим конфиденциальности и не раскрывать информацию лицам, не уполномоченным на ее получение;
- воздерживаться от сделок с ценными бумагами Компании в периоды, определенные внутренними регламентами («тихие периоды»);
- немедленно информировать департамент по связям с инвесторами о любых фактах утечки, несанкционированного доступа или подозрениях на неправомерное использование инсайдерской информации.

Неисполнение требований и (или) нарушение запретов в области ПНИИИМР может повлечь уголовную, административную и гражданско-правовую ответственность в соответствии с применимым законодательством.

Более подробные сведения об обязанностях инсайдеров и соответствующих ограничениях, а также перечень инсайдерской информации общества содержится во внутренних документах, которые размещены на сайте общества по адресу:

<https://softlinegroup.com/investors/disclosure-centrer/>.

ПУБЛИЧНЫЕ КОММУНИКАЦИИ, СОЦИАЛЬНЫЕ СЕТИ И ВЗАИМОДЕЙСТВИЕ СО СМИ

От имени «Софтлайна» вправе выступать только уполномоченные представители. Сотрудники не должны публиковать, комментировать или подтверждать нераскрытую информацию о финансовых результатах, сделках слияния и поглощения, крупных контрактах, стратегических изменениях, продуктовых релизах, инцидентах, клиентах, партнерах или внутренних решениях компании.

При ведении личных социальных сетей сотрудники обязаны отделять свое мнение от позиции Компании, соблюдать конфиденциальность, не использовать бренд «Софтлайна» без разрешения и не распространять непроверенную, дискриминационную, манипулятивную или вводящую в заблуждение информацию.

Контент, созданный с помощью ИИ, должен проходить проверку перед публикацией, если он связан с Компанией, клиентами, продуктами или профессиональной экспертизой сотрудника.

Запросы СМИ, инвесторов, аналитиков, органов власти и иных лиц направляются в уполномоченные службы управления маркетинга, департамента по связям с инвесторами, юридического управления. Самостоятельное предоставление комментариев от имени Компании без полномочий запрещено.

ЗАЩИТА ИНФОРМАЦИИ, ПЕРСОНАЛЬНЫХ ДАННЫХ И КОММЕРЧЕСКОЙ ТАЙНЫ

Настоящее положение определяет ключевые требования к информационной безопасности, защите персональных данных и сохранению коммерческой тайны. Для минимизации рисков и оперативного реагирования на инциденты, каждый сотрудник обязан незамедлительно сообщать обо всех фактах либо подозрениях на утрату, раскрытие или несанкционированный доступ к конфиденциальным активам Компании.

Защита персональных данных

«Софтлайн» обеспечивает приоритетную защиту персональных данных клиентов, партнеров, сотрудников и иных субъектов обработки. Для компании это основа доверия, конфиденциальности, информационной безопасности. Мы строго соблюдаем требования законодательства Российской Федерации и применимых международных стандартов. Защита данных учитывается при проектировании и эксплуатации продуктов, сервисов, ИИ-систем, интеграционных решений и внутренних процессов в соответствии с нормативными требованиями и положениями внутренних документов Группы.

Область применения и определения

Под персональными данными понимаются любые сведения, прямо или косвенно относящиеся к определенному или определяемому физическому лицу (субъекту персональных данных), включая, но не ограничиваясь: ФИО, контактные данные, реквизиты документов, биометрические и технические идентификаторы. Требования распространяются на обработку в любых формах и форматах — автоматизированном и неавтоматизированном, включая использование алгоритмических систем и ИИ-инструментов.

Правовые основания обработки

Обработка персональных данных осуществляется исключительно при наличии хотя бы одного из следующих законных оснований.

- Согласие субъекта на обработку для конкретных, заранее определенных целей.
- Исполнение договора с участием субъекта данных или действий по его запросу до заключения договора.
- Выполнение правовых обязательств, возложенных на «Софтлайн» применимым законодательством.
- Защита жизненно важных интересов субъекта персональных данных.
- Выполнение задач в общественных интересах или в рамках официальных полномочий.
- Обеспечение законных интересов Компании или третьих лиц, за исключением случаев, когда такие интересы превалируют над правами и свободами субъекта (особенно при обработке данных несовершеннолетних).

Обработка данных должна учитывать весь их жизненный цикл: сбор, запись, систематизацию, накопление, использование, передачу и хранение, а также уточнение, блокирование, удаление, обезличивание, уничтожение. Эти же стандарты безопасности распространяются на возможное применение информации в тестировании, аналитике или обучении ИИ-моделей.

Принципы обработки и минимизации данных

Обработка осуществляется с соблюдением принципов законности, целесообразности и минимизации: не допускается обработка персональных данных, избыточных по отношению к заявленным целям обработки. Мы не собираем и не храним данные, если цель обработки можно достичь другими способами. Срок хранения определяется исключительно целями обработки и требованиями применимого законодательства. По достижении целей или истечении срока данные блокируются, а затем удаляются либо обезличиваются.

Меры защиты и конфиденциальность

«Софтлайн» внедряет комплекс правовых, организационных и технических мер для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий. Доступ к данным предоставляется только уполномоченным лицам на основе принципа наименьших привилегий и обязательно контролируется, в том числе регистрируются (логируются) все их действия в информационных системах. Передача данных третьим лицам без согласия субъекта запрещена, за исключением случаев, прямо предусмотренных законодательством или договорными обязательствами с адекватным уровнем защиты.

Клиентские, персональные, конфиденциальные и коммерческие данные не используются для обучения, дообучения, тестирования или улучшения ИИ-моделей без соответствующего правового основания, договорного разрешения, оценки рисков и установленных мер защиты.

Передача персональных данных во внешние облачные сервисы, публичные ИИ-инструменты, API, SaaS-платформы, плагины или расширения браузера допускается только по утвержденным правилам и при соблюдении требований информационной безопасности, конфиденциальности, трансграничной передачи и договорных обязательств.

Права субъектов и комплаенс-контроль

«Софтлайн» обеспечивает субъектам данных возможность реализовать свои права, предусмотренные законодательством, включая право на получение информации об обработке, доступ, исправление, удаление, ограничение обработки и перенос сведений. О любых фактах утечек, незаконной обработки или нарушений режима конфиденциальности необходимо незамедлительно сообщать в службу комплаенса или ответственному за защиту персональных данных. Детальные процедуры регулируются внутренним документом Группы и каждой компании холдинга.

Защита конфиденциальной информации и коммерческой тайны

«Софтлайн» рассматривает **конфиденциальные сведения и коммерческую тайну как стратегические нематериальные активы**, которые формируют конкурентное преимущество и доверие стейкхолдеров. Все сотрудники обязаны обеспечивать сохранность этих данных на протяжении всего цикла обработки, включая этапы сбора, хранения, передачи и архивирования.

Область применения и классификация

Конфиденциальной признается любая информация, не предназначенная для публичного

раскрытия и доступная на условиях неразглашения. Коммерческая тайна включает охраняемые законом внутренние данные, раскрытие которых может нанести ущерб конкурентным позициям или деловой репутации Компании. К охраняемым сведениям относятся:

- персональные данные сотрудников, клиентов и контрагентов;
- финансовые показатели, бюджетные планы, результаты тендеров и переговорных процессов;
- техническая документация, исходный код, архитектурные решения, модели ИИ и результаты внутренних исследований;
- условия сотрудничества с вендорами, клиентские базы, данные о сделках и корпоративной собственности;
- учетные данные, ключи доступа, банковские реквизиты, сведения о компенсациях и льготных программах;
- другие материалы, маркированные как конфиденциальные или подпадающие под действие внутренних политик и договорных обязательств.

Операционные стандарты защиты

Обеспечение конфиденциальности реализуется через комплекс организационных и технических мер.

- **Контроль доступа:** сведения хранятся и обрабатываются исключительно в системах и репозиториях с уровнем доступа, строго соответствующим должностным обязанностям. Вход требует строгой авторизации.
- **Физическая и цифровая гигиена:** обязательное соблюдение политик «чистого стола» и «чистого экрана». При временном отсутствии рабочее место блокируется, бумажные носители размещаются в защищенных хранилищах.
- **Маркировка и безопасная передача:** все конфиденциальные материалы подлежат обязательной классификации и маркировке. Передавать по электронной почте, копировать или печатать их можно только через утвержденные защищенные каналы.
- **Резервирование:** создавать резервные копии можно исключительно в корпоративных системах хранения с применением шифрования для защиты от утраты или повреждения.
- **Ограничение раскрытия:** передавать сведения третьим лицам, включая сотрудников без соответствующего допуска, допускается только при наличии письменного разрешения владельца информации или подписанного соглашения о конфиденциальности.

Запреты

Категорически запрещается разглашать, использовать в личных целях или передавать охраняемые сведения лицам, не имеющим законного права на их получение. Запрещается хранение и передача конфиденциальных данных через персональные устройства или непроверенные внешние сервисы. Любые инциденты, подозрения на утечку или факты несанкционированного доступа должны немедленно фиксироваться и передаваться функции информационной безопасности или комплаенса. Детальные процедуры, включая классификацию данных, инцидент-менеджмент и работу с ИИ-моделями, регулируются регламентом «**О защите конфиденциальной информации**».

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ, КИБЕРБЕЗОПАСНОСТЬ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«Софтлайн» обеспечивает безопасное, законное и этичное использование информационных ресурсов. Это основа цифровой гигиены Компании и защиты корпоративных активов. Требования настоящего стандарта распространяются на все действия сотрудников при использовании корпоративных систем, а также на внешние цифровые активности, если они могут быть ассоциированы с Группой или любой компанией входящей в Группу.

Принципы допустимого использования

Информационные системы, сервисы и устройства Компании используются исключительно в профессиональных целях и в объемах, необходимых для выполнения должностных обязанностей. Запрещается передача через корпоративные каналы связи информации, противоречащей Кодексу, применимому законодательству или внутренним политикам, включая заведомо ложные, дискриминационные, неэтичные или конфиденциальные сведения. При использовании внешних цифровых платформ и ИИ-инструментов сотрудники обязаны соблюдать стандарты конфиденциальности и профессионального поведения.

Контроль доступа и защита учетных данных

Доступ к информационным системам предоставляется на основе принципа наименьших привилегий и требует обязательной авторизации.

Сотрудникам необходимо:

- сохранять конфиденциальность учетных данных (паролей, токенов, ключей доступа) и не передавать их третьим лицам;
 - блокировать сессии во время отсутствия на рабочем месте;
 - использовать многофакторную аутентификацию там, где она предусмотрена;
 - проверять подозрительные письма, ссылки и вложения, а при обнаружении фишинга или вредоносного ПО — немедленно сообщать об этом специалистам;
- информировать службу информационной безопасности о любых признаках несанкционированного доступа или компрометации учетной записи.

Сотрудники не должны:

- обходить настройки безопасности и отключать защитные средства;
- подключать несанкционированные устройства и облачные хранилища, устанавливать сторонние плагины и расширения браузера;
- использовать внешние программные интерфейсы приложений, облачные или ИИ-сервисы для обработки корпоративных, клиентских или персональных данных без согласования.

Лицензионная дисциплина и управление программным обеспечением

Сотрудники могут использовать программное обеспечение строго в рамках лицензионных соглашений и корпоративных стандартов. Запрещается без предварительного письменного согласования с уполномоченными подразделениями:

- устанавливать программное обеспечение на корпоративное оборудование;
- размещать корпоративное или лицензионное ПО на персональных или сторонних устройствах;
- копировать, распространять или передавать третьим лицам копии программного обеспечения, принадлежащего Компании или используемого на лицензионной основе.

Ответственность

Нарушение настоящих стандартов квалифицируется как дисциплинарное правонарушение, которое может привести к ограничению доступа к информационным ресурсам, дисциплинарным взысканиям или прекращению трудовых отношений. Регулярный аудит использования ПО и мониторинг цифровых активностей обеспечивают соблюдение лицензионных требований и предотвращает утечки. Детальные процедуры регулируются внутренними регламентами по информационной безопасности и управлению ИТ-активами.

ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ И ОТКРЫТЫЙ ИСХОДНЫЙ КОД

«Софтлайн» уважает права на интеллектуальную собственность клиентов, сотрудников, поставщиков, партнеров, авторов проектов с открытым исходным кодом и других лиц. Код, архитектурные решения, документация, модели, наборы данных, задачи для генеративных моделей, обучающие материалы, дизайн, коммерческие предложения и иные результаты интеллектуальной деятельности Компания использует только при наличии правового основания и в соответствии с договорными условиями.

Запрещается копировать, распространять, включать в продукты или клиентские решения программный код, данные, изображения, тексты, модели, библиотеки, программные интерфейсы приложений, наборы данных или результаты генеративного ИИ без проверки прав, лицензий, ограничений на коммерческое использование, требований атрибуции, условий распространения и рисков раскрытия исходного кода.

Использование программного обеспечения с открытым исходным кодом и внешних ИИ-моделей должно проходить оценку лицензий, информационной безопасности, совместимости с продуктовой архитектурой, рисков привязки к поставщику, требований клиента и возможного влияния на права «Софтлайна» и третьих лиц.

Исключительные права на результаты интеллектуальной деятельности, в том числе на программы для ЭВМ, базы данных, произведения, изобретения, полезные модели и промышленные образцы, созданные работником в рамках его трудовых обязанностей или по конкретному заданию работодателя, принадлежат Компании, если трудовым или иным договором между работником и «Софтлайном» не предусмотрено иное.

Работник обязан письменно уведомлять «Софтлайн» о созданных служебных результатах, воздерживаться от их самостоятельного использования и раскрытия и содействовать оформлению, государственной регистрации и защите прав Компании. Порядок выявления и учета служебных результатов, а также выплаты работнику вознаграждения определяется Кодексом по интеллектуальной собственности и другими внутренними документами.

Сведения, в отношении которых установлен режим коммерческой тайны, включая секреты производства (ноу-хау), а также иная конфиденциальная информация (исходный код, технические и организационные решения, методики, сведения о клиентах, контрагентах и финансовых показателях) находятся под охраной.

Работник обязан соблюдать установленный режим коммерческой тайны, не разглашать такие сведения, не использовать их вне исполнения трудовых обязанностей и не передавать третьим лицам без правового основания. Эта обязанность сохраняется в течение всего срока действия режима коммерческой тайны, в том числе после прекращения трудовых или других договорных отношений с «Софтлайном».

Сотрудникам запрещено раскрывать охраняемую информацию при публичных выступлениях, в публикациях, средствах массовой информации, социальных сетях, открытых хранилищах исходного кода и профессиональных сообществах. Размещение в открытом доступе исходного кода, технической документации, сведений о клиентах и проектах, а также изображений внутренних информационных систем Компании допускается только при наличии правового основания и предварительного согласования в установленном порядке.

Работники не вправе выдавать результаты интеллектуальной деятельности третьих лиц (программный код, тексты, иные материалы и исследования, в том числе созданные с использованием систем искусственного интеллекта) за результаты собственного труда и обязаны указывать авторство и источники материалов в соответствии с условиями их правомерного использования.

Работники не используют при исполнении трудовых обязанностей объекты интеллектуальной собственности и сведения, составляющие коммерческую тайну прежних работодателей и иных третьих лиц, при отсутствии правового основания и не включают такие объекты и сведения в материалы и продукты «Софтлайна».

Этот раздел устанавливает общие правила поведения работников в сфере интеллектуальной собственности. Детальные требования к созданию, выявлению, учету, правовой охране, применению и защите результатов интеллектуальной деятельности, а также к правомерному использованию программного обеспечения с открытым исходным кодом определяются Кодексом по интеллектуальной собственности и другими внутренними документами Компании.

ОТВЕТСТВЕННОЕ ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И НОВЫХ ТЕХНОЛОГИЙ

«Софтлайн» использует искусственный интеллект как инструмент усиления экспертизы человека, повышения качества решений и создания ценности для клиентов, сотрудников и общества. Кодекс задает общий поведенческий стандарт работы с ИИ. Детальные требования к разработке, внедрению, эксплуатации, аудиту, контролю качества, управлению рисками и реагированию на инциденты устанавливаются Кодексом ответственной разработки и использования ИИ, Политикой обеспечения соответствия требованиям в области ИИ, глоссарием и другими внутренними регламентами.

Требования раздела распространяются на собственную продуктовую и заказную разработку, интеграционные проекты для клиентов, консультирование, внутреннее использование ИИ сотрудниками, внешние ИИ-сервисы, программные интерфейсы приложений, облачные платформы, локальные модели, модели с открытым исходным кодом и иные технологические инструменты с ИИ-компонентами.

Принципы ответственного ИИ

При разработке, закупке, внедрении и использовании ИИ «Софтлайн» руководствуется принципами человекоцентричности и пользы, справедливости и недискриминации, прозрачности и объяснимости, надежности и безопасности, конфиденциальности и защиты данных, подотчетности и человеческого контроля, устойчивого развития и разумного использования вычислительных ресурсов.

Правила для сотрудников

Сотрудники обязаны:

- использовать ИИ только для законных, этических и деловых целей;
- не передавать в неутвержденные ИИ-сервисы персональные данные, коммерческую тайну, клиентские данные, исходный код, договорные материалы, финансовую информацию, учетные данные и иные конфиденциальные сведения;
- проверять значимые результаты ИИ перед использованием;
- не выдавать результат ИИ за экспертную проверку, если такая проверка не проводилась.

Использование ИИ не снимает ответственности с сотрудника, руководителя, проектной команды или компании за результат, рекомендацию, документ или действие. Решения, способные повлиять на права, занятость, здоровье, безопасность, финансы, доступ к услугам или существенные интересы человека, не должны приниматься автоматически без надлежащего человеческого контроля и возможности пересмотра.

Клиентские проекты и риск-ориентированный подход

В клиентских проектах компания обеспечивает прозрачное информирование о существенном использовании ИИ, ограничениях модели, требованиях к данным, рисках эксплуатации и распределении ответственности между «Софтлайном», клиентом и поставщиками технологий. Чем выше влияние ИИ-системы на права человека, безопасность, финансы, занятость, критическую инфраструктуру, персональные данные

или доверие клиента, тем выше требования к предварительной оценке рисков, документированию, тестированию, валидации, мониторингу и человеческому контролю.

Недопустимые применения

Сотрудникам Компании запрещается разрабатывать, продавать, внедрять или использовать ИИ:

- для незаконного наблюдения и скрытой манипуляции общественным мнением;
- для создания вредоносного ПО или инструментов компьютерных атак;
- для незаконного сбора биометрии и принятия дискриминационных решений;
- для создания поддельных материалов — изображений, видео, аудио — для дезинформации;
- для развертывания автономных систем без участия человека, а также полностью автономных решений в критически важных сферах без человеческого контроля.

Инциденты, связанные с ИИ, и реагирование на них

Сотрудники обязаны незамедлительно сообщать через установленные каналы о случаях утечки данных через ИИ-инструменты, дискриминационных или опасных результатах модели, некорректном автоматизированном решении, несанкционированном использовании клиентских данных, генерации вредоносного кода, поддельных материалов, дезинформации, сбое ИИ-системы или ином событии, способном повлиять на клиента, безопасность, права людей или репутацию «Софтлайна».

ЭКОЛОГИЧЕСКАЯ И СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ (ESG)

«Софтлайн» интегрирует принципы устойчивого развития в стратегию и операционную деятельность и принимает на себя ответственность за экологические и социальные последствия бизнеса.

Экологические обязательства и ответственное потребление

Компания минимизирует негативное воздействие на окружающую среду: выбирает ресурсосберегающие технологии, оптимизирует операционные процессы и внедряет стандарты «зеленого» офиса. Мы способствуем экологической трансформации рынка, предлагая клиентам цифровые решения и ИИ-инструменты для повышения энергоэффективности, снижения углеродного следа и рационального управления ресурсами.

Это также включает энергоэффективность ИТ-инфраструктуры, экологический след дата-центров и ИИ, ответственное проектирование цифровых решений, доступность технологий, разумное использование вычислительных ресурсов и поддержку развития компетенций сотрудников в условиях автоматизации.

Приоритет отдается проектам и партнерам, разделяющим принципы устойчивого развития.

Социальные инвестиции и развитие человеческого капитала

«Софтлайн» развивает программы корпоративного волонтерства и благотворительности с фокусом на поддержку уязвимых групп: защиту прав детей, помощь детям с инвалидностью, укрепление общественного здоровья. В области управления талантами Компания создает инклюзивную среду, равные возможности для профессионального роста и оказывает адресную поддержку сотрудникам, оказавшимся в сложных жизненных обстоятельствах.

СООБЩЕНИЕ О НАРУШЕНИЯХ, РАССЛЕДОВАНИЯ И ЗАЩИТА ОТ ПРЕСЛЕДОВАНИЯ

«Софтлайн» поддерживает культуру открытого диалога: если сотрудник сталкивается с поведением, решением, поручением или практикой, которые вызывают сомнение с точки зрения закона, этики, безопасности, защиты данных, ИИ, конфликта интересов, коррупции или уважительной рабочей среды, он должен обратиться за консультацией или сообщить о ситуации.

Сообщение по вопросам комплаенс направляется руководителю и в юридическое управление: [**compliance@softline.com**](mailto:compliance@softline.com)

Сообщение по вопросам безопасности направляется руководителю и в управление безопасности: [**corpsecurity@softline.com**](mailto:corpsecurity@softline.com)

Своевременное информирование позволяет исправить ситуацию до того, как она приведет к нарушению закона, утечке данных, нанесет ущерб клиенту и репутации Компании. «Софтлайн» гарантирует конфиденциальность личности заявителя в максимально возможной степени, допускаемой законом, и проводит объективное, беспристрастное и конфиденциальное рассмотрение сообщений.

Сотрудник защищен, если добросовестно сообщает о возможном нарушении или участвует в расследовании, даже если факт нарушения впоследствии не подтвердится. Запрещены любые формы преследования, включая увольнение, понижение в должности, ухудшение оценки, лишение проектов, изоляцию, угрозы, давление через коллег, отказ в повышении, дискриминацию или иные негативные последствия.

Заведомо ложные сообщения, фабрикация доказательств, сокрытие существенной информации или злоупотребление каналами информирования могут рассматриваться как нарушение Кодекса. Во время внутренних расследований сотрудники обязаны помогать Компании, отвечать на вопросы честно, своевременно и максимально полно.

Ответственность за нарушения

Нарушение положений Кодекса может повлечь дисциплинарные меры в соответствии с трудовым законодательством и внутренними документами Компании, включая расторжение трудового договора. Если действия содержат признаки административного правонарушения или преступления, материалы могут быть переданы в уполномоченные органы.

Мера воздействия определяется с учетом характера нарушения, последствий, умысла, повторности, уровня должности, сотрудничества с расследованием, добровольного сообщения, возмещения ущерба и наличия смягчающих или отягчающих обстоятельств. Наказание применяется независимо от должности, стажа и заслуг сотрудника.

Руководители несут ответственность не только за собственные нарушения, но и за игнорирование сигналов, давление на сотрудников, создание культуры результата любой ценой, игнорирование очевидных рисков, сокрытие нарушений или преследование заявителей.

Помимо дисциплинарных мер, Компания может применять корректирующие действия: дополнительное обучение, изменение процесса, усиление контроля, пересмотр

полномочий, ограничение доступа, изменение условий взаимодействия с контрагентом или прекращение отношений с ним.

Подтверждение ознакомления и обучение сотрудников

Все новые сотрудники обязаны ознакомиться с Кодексом в течение 5 рабочих дней с момента приема на работу под роспись, в т.ч. электронную.

Группа проводит регулярное обучение по этике, противодействию коррупции, информационной безопасности, защите данных. Базовое тестирование по материалам Кодекса является обязательным и проводится не реже одного раза в два года. Для отдельных ролей предусмотрено углубленное обучение.

Пересмотр документа

Кодекс пересматривается не реже одного раза в два года, а также при существенных изменениях законодательства, структуры Группы, профиля рисков, технологий, требований клиентов, регуляторных ожиданий или внутренних политик. Владелец документа является юридическое управление (функция комплаенса) совместно с управлением персоналом. Кодекс утверждается Советом директоров ПАО «Софтлайн» после предварительного рассмотрения Правлением ПАО «Софтлайн». Учет версии, дата следующего пересмотра и перечень связанных политик фиксируются в установленном порядке.