Корпоративная политика управления данными и информационной безопасности

Версия 1.0 - 18 апреля 2025 г.

1. ВВЕДЕНИЕ

1.1 Цель документа

Настоящая Корпоративная политика управления данными и информационной безопасности ("Политика") устанавливает основные принципы, требования и правила обращения с корпоративной информацией в ООО "ТехноИнновация" (далее - "Компания"). Политика разработана для обеспечения надлежащей защиты данных, соблюдения нормативных требований и минимизации рисков информационной безопасности.

1.2 Область применения

Действие настоящей Политики распространяется на всех сотрудников Компании, включая временных работников, консультантов, подрядчиков и деловых партнеров, имеющих доступ к корпоративным информационным системам. Политика охватывает все данные, создаваемые, получаемые, хранимые и обрабатываемые Компанией, независимо от формата и местонахождения.

1.3 Законодательная база

Настоящая Политика разработана в соответствии со следующими нормативно-правовыми актами:

•Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
•Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
•Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ
•Международный стандарт ISO/IEC 27001:2013 "Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности"
•Иные применимые нормативно-правовые акты Российской Федерации

2. КЛАССИФИКАЦИЯ ИНФОРМАЦИИ

2.1 Категории данных

В рамках настоящей Политики информация, обрабатываемая Компанией, классифицируется по следующим категориям:**2.1.1 Публичная информация** Информация, которая официально одобрена руководством Компании для публичного распространения и не требует специальных мер защиты. Примеры: маркетинговые материалы, общедоступная информация о продуктах и услугах, пресс-релизы.**2.1.2 Внутренняя информация** Информация для внутреннего

использования, несанкционированное раскрытие которой может нанести репутационный ущерб Компании или создать неудобства в операционной деятельности. Примеры: внутренние процедуры, регламенты, корпоративные телефонные справочники, организационные диаграммы.**2.1.3 Конфиденциальная информация** Информация ограниченного доступа, несанкционированное раскрытие которой может привести к финансовым потерям или правовым последствиям. Примеры: финансовые отчеты, данные клиентов, интеллектуальная собственность, коммерческие договоры.**2.1.4 Строго конфиденциальная информация** Критически важная информация, требующая максимального уровня защиты, несанкционированное раскрытие которой может привести к значительному ущербу для Компании. Примеры: стратегические планы развития, патенты в разработке, исходные коды программного обеспечения.

2.2 Маркировка данных

Все документы и файлы, содержащие конфиденциальную и строго конфиденциальную информацию, должны быть соответствующим образом маркированы. Маркировка должна быть четкой, заметной и включать следующую информацию:

•Уровень конфиденциальности
•Владелец информации
•Дата создания/обновления
•Срок действия грифа конфиденциальности (если применимо)

2.3 Пересмотр классификации

Владельцы информационных активов обязаны периодически (не реже одного раза в год) пересматривать классификацию подконтрольных им данных и вносить необходимые изменения в соответствии с актуальными бизнес-требованиями и оценкой рисков.

3. УПРАВЛЕНИЕ ДОСТУПОМ

3.1 Принципы управления доступом

Доступ к информационным системам и данным Компании основывается на следующих принципах:

•**Принцип минимальных привилегий**: сотрудники получают только тот уровень доступа, который необходим для выполнения их должностных обязанностей
•**Разделение обязанностей**: критические функции распределяются между разными сотрудниками для предотвращения конфликта интересов и мошеннических действий
•**Обоснованность доступа**: доступ предоставляется только при наличии документально оформленной служебной необходимости
•**Периодический пересмотр**: права доступа регулярно пересматриваются и обновляются

3.2 Управление учетными записями

Все пользователи информационных систем должны иметь индивидуальные учетные записи. Запрещается совместное использование учетных данных. Процесс управления учетными записями включает:

•Создание учетных записей на основании официальных запросов, согласованных с руководителями подразделений
•Временное блокирование учетных записей при длительном отсутствии сотрудника (отпуск, больничный более 30 дней)
•Немедленная деактивация учетных записей при увольнении сотрудника или изменении его должностных обязанностей
•Регулярный аудит активных учетных записей и их привилегий (не реже одного раза в квартал)

3.3 Парольная политика

В целях обеспечения безопасности доступа к информационным системам Компании устанавливаются следующие требования к паролям:

•Минимальная длина пароля – 12 символов
•Обязательное использование символов из различных категорий: прописные и строчные буквы, цифры, специальные символы
•Срок действия пароля – не более 90 дней
•Запрет на повторное использование последних 12 паролей
•Блокировка учетной записи после 5 неудачных попыток ввода пароля
•Запрет на использование в паролях личной информации (имена, даты рождения и т.п.)
•Хранение паролей только в зашифрованном виде

3.4 Многофакторная аутентификация

Доступ к критическим системам и данным (финансовые системы, системы разработки, административный доступ) должен осуществляться с использованием многофакторной аутентификации. В качестве второго фактора могут использоваться:

•Аппаратные токены
•Мобильные приложения для генерации одноразовых паролей
•SMS-коды или push-уведомления
•Биометрические данные (при наличии технической возможности)

4. ЗАЩИТА ДАННЫХ

4.1 Защита данных при хранении

Для обеспечения безопасности хранимых данных применяются следующие меры:

•Шифрование конфиденциальных и строго конфиденциальных данных на всех носителях информации
•Сегментирование сетей хранения данных в соответствии с их классификацией

•Резервное копирование всех критических данных не реже одного раза в сутки
•Физическая защита серверных помещений и хранилищ резервных копий
•Защита от вредоносного программного обеспечения с регулярным обновлением антивирусных баз
•Своевременная установка обновлений безопасности для всех систем хранения данных

4.2 Защита данных при передаче

При передаче данных внутри и за пределы корпоративной сети должны соблюдаться следующие требования:

•Использование защищенных протоколов передачи данных (HTTPS, SFTP, SCP и др.)
•Шифрование конфиденциальных данных перед их передачей по незащищенным каналам связи
•Использование виртуальных частных сетей (VPN) при удаленном доступе к корпоративным ресурсам
•Контроль и фильтрация сетевого трафика с помощью межсетевых экранов
•Обнаружение и предотвращение сетевых вторжений
•Регулярный мониторинг сетевой активности и выявление аномалий

4.3 Управление мобильными устройствами

Использование мобильных устройств (ноутбуки, планшеты, смартфоны) для доступа к корпоративным данным регламентируется следующими правилами:

•Все мобильные устройства, используемые для работы с корпоративными данными, должны быть зарегистрированы в системе управления мобильными устройствами (MDM)
•Обязательное шифрование корпоративных данных на мобильных устройствах
•Настройка автоматической блокировки экрана после периода неактивности (не более 5 минут)
•Возможность удаленной очистки корпоративных данных в случае утери или кражи устройства
•Запрет на установку непроверенного программного обеспечения на устройства с доступом к корпоративным данным
•Регулярные обновления операционных систем и приложений

4.4 Удаление и уничтожение данных

По истечении установленных сроков хранения или при отсутствии необходимости в дальнейшем использовании, данные должны быть надежно удалены или уничтожены в соответствии со следующими требованиями:

•Использование специализированного программного обеспечения для необратимого удаления данных с электронных носителей
•Физическое уничтожение носителей информации, не подлежащих повторному использованию
•Документирование процесса уничтожения конфиденциальных и строго конфиденциальных данных
•Проверка эффективности процедур удаления данных с целью предотвращения возможности их восстановления

5. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Общие положения

Обработка персональных данных в Компании осуществляется с соблюдением принципов и правил, установленных Федеральным законом "О персональных данных" от 27.07.2006 N 152-ФЗ. Компания гарантирует конфиденциальность и безопасность обрабатываемых персональных данных.

5.2 Сбор и обработка персональных данных

При сборе и обработке персональных данных должны соблюдаться следующие принципы:

•Получение предварительного согласия субъекта персональных данных на их обработку
•Ограничение объема собираемых данных минимально необходимым для достижения заявленных целей
•Обеспечение точности, достаточности и актуальности персональных данных
•Соблюдение целевого ограничения при обработке персональных данных
•Прозрачность процессов обработки персональных данных для субъектов персональных данных

5.3 Передача персональных данных

Передача персональных данных третьим лицам возможна только в следующих случаях:

•С согласия субъекта персональных данных
•По требованию уполномоченных государственных органов
•В рамках исполнения договорных обязательств, если это предусмотрено соответствующим договором
•В иных случаях, установленных законодательством РФ

При передаче персональных данных третьим лицам Компания обязуется заключать соответствующие соглашения о конфиденциальности и обеспечении безопасности передаваемых данных.

5.4 Хранение и уничтожение персональных данных

Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки, если срок хранения не установлен федеральным законом или договором. Уничтожение персональных данных производится:

•По достижении целей обработки
•При отзыве субъектом персональных данных согласия на их обработку
•По истечении установленных сроков хранения
•В случае выявления неправомерной обработки персональных данных

6. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

6.1 Организация информационной безопасности

В Компании создается и поддерживается организационная структура информационной безопасности, включающая:

•Комитет по информационной безопасности под председательством Генерального директора
•Департамент информационной безопасности, возглавляемый Директором по информационной безопасности (CISO)
•Ответственных за информационную безопасность в каждом структурном подразделении
•Рабочую группу по реагированию на инциденты информационной безопасности

6.2 Управление инцидентами безопасности

В Компании разрабатывается и внедряется система управления инцидентами информационной безопасности, включающая:

•Процедуры выявления и регистрации инцидентов
•Классификацию инцидентов по уровням критичности
•Порядок эскалации и информирования о инцидентах
•Процедуры расследования причин инцидентов
•Меры по устранению последствий инцидентов и предотвращению их повторения
•Документирование всех действий по обработке инцидентов

6.3 Антивирусная защита

Для защиты от вредоносного программного обеспечения в Компании применяются следующие меры:

•Установка антивирусного программного обеспечения на всех рабочих станциях и серверах
•Автоматическое обновление антивирусных баз данных
•Периодическое полное сканирование информационных систем
•Проверка входящих файлов на наличие вирусов
•Блокировка доступа к потенциально опасным веб-сайтам
•Запрет на использование неавторизованного программного обеспечения

6.4 Аудит и мониторинг

Для своевременного выявления потенциальных угроз и нарушений безопасности в Компании организован постоянный мониторинг и аудит информационных систем:

•Сбор и анализ журналов событий безопасности всех критических систем
•Мониторинг сетевого трафика и выявление аномалий
•Контроль целостности системных файлов и конфигураций
•Регулярные проверки на наличие уязвимостей в информационных системах
•Периодические тесты на проникновение
•Анализ соответствия настроек систем требованиям безопасности

6.5 Управление уязвимостями

В Компании внедрен процесс управления уязвимостями, включающий:

•Регулярное сканирование информационных систем на наличие уязвимостей
•Оценку критичности выявленных уязвимостей
•Приоритизацию устранения уязвимостей на основе оценки рисков
•Своевременную установку обновлений безопасности
•Тестирование обновлений перед внедрением в производственную среду
•Мониторинг информации о новых уязвимостях из достоверных источников

7. ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ БИЗНЕСА

7.1 План обеспечения непрерывности бизнеса

Компания разрабатывает и поддерживает в актуальном состоянии План обеспечения непрерывности бизнеса (BCP), включающий:

•Анализ влияния на бизнес (BIA) для определения критических бизнес-процессов и систем
•Оценку рисков прерывания бизнес-процессов
•Стратегии восстановления для различных сценариев
•Планы коммуникаций в кризисных ситуациях
•Распределение ролей и ответственности при активации плана
•Процедуры возврата к нормальной работе после устранения инцидента

7.2 План аварийного восстановления

В рамках обеспечения непрерывности бизнеса разрабатывается План аварийного восстановления (DRP), определяющий:

•Приоритеты восстановления информационных систем
•Целевое время восстановления (RTO) и целевую точку восстановления (RPO) для каждой критической системы
•Технические процедуры восстановления систем и данных
•Альтернативные площадки для размещения ИТ-инфраструктуры
•Процедуры тестирования возможности восстановления систем и данных

7.3 Резервное копирование

Система резервного копирования Компании организована согласно следующим принципам:

•Определение объектов резервного копирования на основе их критичности
•Разработка графиков резервного копирования с учетом требований к сохранности данных
•Использование многоуровневой стратегии резервного копирования (полное, дифференциальное, инкрементное)
•Хранение резервных копий в географически удаленных местах
•Регулярная проверка целостности и возможности восстановления из резервных копий
•Защита резервных копий с помощью шифрования

7.4 Тестирование планов

Планы обеспечения непрерывности бизнеса и аварийного восстановления подлежат регулярному тестированию:

•Настольные учения (table-top exercises) – не реже одного раза в полугодие
•Функциональное тестирование отдельных компонентов – не реже одного раза в квартал
•Полное тестирование с симуляцией реальных сценариев – не реже одного раза в год
•Тестирование восстановления из резервных копий – ежемесячно
•Актуализация планов по результатам тестирования и при существенных изменениях в ИТ-инфраструктуре

8. ОБУЧЕНИЕ И ОСВЕДОМЛЕННОСТЬ

8.1 Программа обучения по информационной безопасности

В Компании разрабатывается и реализуется комплексная программа обучения сотрудников по вопросам информационной безопасности:

•Обязательное вводное обучение для новых сотрудников
•Регулярные тренинги для всех сотрудников (не реже одного раза в год)
•Специализированные курсы для ИТ-персонала и сотрудников, работающих с конфиденциальной информацией
•Дополнительные тренинги при внедрении новых систем или изменении политик безопасности

8.2 Повышение осведомленности

Для повышения осведомленности сотрудников в вопросах информационной безопасности используются следующие методы:

•Регулярные информационные рассылки о актуальных угрозах и методах защиты
•Публикация материалов по информационной безопасности на корпоративном портале
•Проведение дней информационной безопасности
•Размещение наглядных материалов (плакаты, памятки) в офисных помещениях
•Симуляции фишинговых атак с последующим разбором результатов

8.3 Оценка эффективности

Эффективность программ обучения и повышения осведомленности оценивается на основе:

•Результатов тестирования знаний сотрудников
•Статистики инцидентов безопасности, связанных с человеческим фактором
•Результатов симуляций социальной инженерии
•Обратной связи от сотрудников
•Соответствия поведения сотрудников требованиям политик безопасности

9. СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

9.1 Соблюдение законодательства

Компания обязуется соблюдать все применимые законодательные и нормативные требования в области информационной безопасности и защиты данных. Департамент информационной безопасности совместно с юридическим департаментом осуществляет:

•Мониторинг изменений в законодательстве и нормативных требованиях
•Оценку влияния этих изменений на деятельность Компании
•Адаптацию политик и процедур для обеспечения соответствия новым требованиям
•Проведение регулярных проверок на соответствие требованиям

9.2 Внутренний аудит

Программа внутреннего аудита информационной безопасности включает:

•Регулярные проверки соответствия практик управления информационной безопасностью требованиям настоящей Политики
•Оценку эффективности мер контроля информационной безопасности
•Выявление областей для улучшения
•Разработку рекомендаций по устранению выявленных недостатков
•Контроль выполнения корректирующих мероприятий

9.3 Внешний аудит

По решению руководства Компании могут проводиться внешние аудиты информационной безопасности с привлечением специализированных организаций для:

•Независимой оценки состояния информационной безопасности
•Подтверждения соответствия международным стандартам и лучшим практикам
•Подготовки к сертификации по стандартам информационной безопасности
•Выполнения специальных требований клиентов или партнеров

10. ОТВЕТСТВЕННОСТЬ И ДИСЦИПЛИНАРНЫЕ МЕРЫ

10.1 Ответственность сотрудников

Все сотрудники Компании несут персональную ответственность за:

•Соблюдение требований настоящей Политики и связанных с ней процедур
•Защиту конфиденциальной информации от несанкционированного доступа
•Своевременное информирование о инцидентах информационной безопасности
•Рациональное использование ресурсов информационных систем
•Соблюдение правил использования средств защиты информации

10.2 Дисциплинарные меры

За нарушение требований настоящей Политики могут применяться следующие дисциплинарные меры:

•Устное предупреждение
•Письменное замечание
•Временное ограничение доступа к информационным системам
•Лишение премий и иных поощрительных выплат
•Дисциплинарное взыскание в соответствии с трудовым законодательством
•В случае серьезных нарушений - расторжение трудового договора

Степень дисциплинарной ответственности зависит от тяжести нарушения, умысла, последствий и других обстоятельств инцидента.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1 Утверждение и введение в действие

Настоящая Политика утверждается Генеральным директором Компании и вводится в действие приказом.

11.2 Пересмотр и актуализация

Политика подлежит пересмотру и актуализации не реже одного раза в год, а также в случае существенных изменений в организационной структуре Компании, ИТ-инфраструктуре, законодательстве или условиях ведения бизнеса.

11.3 Контроль исполнения

Контроль исполнения требований настоящей Политики возлагается на Директора по информационной безопасности.

11.4 Действие Политики

Настоящая Политика действует с момента утверждения до момента ее отмены или замены новой версией.