



команда роста на аутсорсе
для системного улучшения ключевых метрик

Шаблон политики использования корпоративного VPN и удаленного доступа

Стандартизация подхода к информационной безопасности при удаленной работе

Введение

Настоящий документ определяет правила и процедуры использования корпоративной виртуальной частной сети (VPN) и удаленного доступа к информационным ресурсам компании. Целью является обеспечение конфиденциальности, целостности и доступности корпоративных данных, а также минимизация рисков информационной безопасности при работе вне офиса.

Данная Политика обязательна для ознакомления и исполнения всеми сотрудниками, подрядчиками и сторонними организациями, имеющими доступ к корпоративным информационным системам компании.

Общие положения

VPN (Virtual Private Network)	Виртуальная частная сеть, обеспечивающая защищенное зашифрованное соединение между устройством пользователя и корпоративной сетью через общедоступные сети (например, Интернет).
Удаленный доступ	Возможность подключения к корпоративным информационным системам и ресурсам извне корпоративной сети.
Конфиденциальная информация	Любая информация, доступ к которой ограничен законодательством РФ (например, 152-ФЗ «О персональных данных») или внутренними нормативными документами компании (коммерческая тайна, персональные данные сотрудников и клиентов, финансовая информация, интеллектуальная собственность).
Ответственность сотрудников	Каждый сотрудник несет персональную ответственность за соблюдение данной Политики и защиту корпоративных данных, к которым он имеет доступ. Несоблюдение Политики может повлечь дисциплинарные взыскания, вплоть до увольнения, и/или юридическую ответственность.

Требования к устройствам

- ☐ Использование корпоративных устройств для доступа к конфиденциальной информации

Приоритет отдается корпоративным устройствам. Использование личных устройств допускается только с разрешения ИТ-отдела и при условии соответствия всем требованиям безопасности.

☐ **Операционная система**

Должна быть актуальной версии (например, Windows 10/11, macOS не старше 2-х последних версий, актуальные версии iOS/Android) и регулярно обновляться.

☐ **Антивирусное программное обеспечение**

Обязательно наличие лицензионного антивирусного ПО с актуальными базами данных и активной защитой в реальном времени.

☐ **Автоматические обновления**

Включены автоматические обновления операционной системы и всего установленного ПО.

☐ **Брандмауэр (файервол)**

Включен и настроен на устройстве.

☐ **Запрещенное программное обеспечение**

На устройствах, используемых для удаленного доступа к корпоративным ресурсам, запрещено устанавливать нелицензионное ПО, торрент-клиенты, анонимайзеры, публичные VPN-сервисы, а также любое ПО, не одобренное ИТ-отделом.

Правила использования VPN

☐ **Обязательность использования VPN**

Для доступа к любым корпоративным ресурсам (CRM, ERP, файловые серверы, корпоративная почта и т.д.) извне корпоративной сети обязательно использование корпоративного VPN.

☐ **Запрет на использование публичных VPN-сервисов**

Использование сторонних, не корпоративных VPN-сервисов для доступа к корпоративным ресурсам строго запрещено.

☐ **Правила поведения в публичных Wi-Fi сетях**

При работе в публичных Wi-Fi сетях (кафе, аэропорты, отели) обязательно использование корпоративного VPN. Запрещено передавать конфиденциальную информацию до установления VPN-соединения. Избегайте подключения к сетям без пароля или с подозрительными названиями.

☐ **Многофакторная аутентификация (MFA)**

Для подключения к корпоративному VPN обязательна многофакторная аутентификация (MFA). Это может быть SMS-код, приложение-аутентификатор или аппаратный токен.

☐ **Раздельное туннелирование (Split Tunneling)**

Для оптимизации производительности и снижения нагрузки на VPN-сервер может использоваться раздельное туннелирование: только трафик к корпоративным ресурсам проходит через VPN, остальной трафик идет напрямую в Интернет.

Политика паролей

Сложность пароля

Минимум 12 символов, включающих заглавные и строчные буквы, цифры и специальные символы. Не должен содержать личную информацию или легко угадываемые слова.

Периодичность смены

Пароли должны меняться не реже одного раза в 90 дней.

Хранение паролей

Пароли должны храниться в зашифрованном виде (например, в менеджере паролей) или запоминаться. Запрещено записывать пароли на бумаге, хранить в незашифрованных файлах или передавать третьим лицам.

Уникальность паролей

Запрещено использовать один и тот же пароль для разных корпоративных систем или для корпоративных и личных аккаунтов.

Доступ к информации

☐ Принцип минимальных привилегий

Сотрудникам предоставляется доступ только к тем информационным ресурсам и данным, которые необходимы для выполнения их должностных обязанностей.

☐ Классификация данных

Все корпоративные данные классифицируются как: конфиденциальные (строго ограниченный доступ), внутренние (доступ для сотрудников компании), публичные (доступ без ограничений).

☐ Работа с конфиденциальными данными вне офиса

Запрещено хранить конфиденциальные данные на личных устройствах или в облачных хранилищах, не одобренных компаний. При работе с конфиденциальной информацией в общественных местах необходимо обеспечить конфиденциальность экрана (использование защитных пленок, выбор места).

☐ Передача данных

Передача конфиденциальных данных третьим лицам разрешена только через защищенные каналы связи и с письменного согласия руководства.

Действия в случае инцидента

☐ Подозрение на компрометацию устройства/учетных данных

Немедленно сообщить в ИТ-отдел о любых подозрениях на взлом, потерю устройства, несанкционированный доступ к учетным данным или необычную активность.

☐ Процедура сообщения об инциденте

Сотрудник должен связаться с ИТ-отделом по телефону: [Указать номер] или по электронной почте: [Указать адрес]. В сообщении указать ФИО, должность, описание инцидента, дату и время обнаружения.

☐ Ответственность за несоблюдение политик

Несообщение об инциденте или умышленное нарушение данной Политики может повлечь за собой дисциплинарные взыскания, вплоть до увольнения, и/или юридическую ответственность в соответствии с законодательством РФ.

Мониторинг и аудит

Компания оставляет за собой право осуществлять мониторинг VPN-трафика, активности пользователей и состояния устройств, подключенных к корпоративной сети через VPN. Это включает, но не ограничивается, запись журналов подключений, объемов передаваемых данных, посещаемых ресурсов и используемых приложений. Мониторинг проводится исключительно в целях обеспечения информационной безопасности, соблюдения данной Политики и предотвращения инцидентов. Все данные мониторинга являются конфиденциальными и используются в соответствии с законодательством РФ.

Обучение и информирование

☐ Обязанность сотрудника по ознакомлению

Каждый сотрудник обязан ознакомиться с данной Политикой и подтвердить свое согласие с ее условиями.

☐ Регулярное обучение

Компания проводит регулярные тренинги и инструктажи по вопросам информационной безопасности и правилам использования VPN. Участие в таких мероприятиях является обязательным.

☐ Актуализация Политики

Данная Политика может быть изменена или дополнена. Сотрудники будут уведомлены о любых изменениях и обязаны ознакомиться с актуальной версией.

Приложения

Приложение 1: Форма согласия сотрудника с Политикой использования корпоративного VPN и удаленного доступа.

[Название компании]

СОГЛАСИЕ СОТРУДНИКА

с Политикой использования корпоративного VPN и удаленного доступа

Я, [ФИО сотрудника], [Должность], подтверждаю, что ознакомлен(а) с «Политикой использования корпоративного VPN и удаленного доступа» компании [Название компании], понимаю ее положения и обязуюсь неукоснительно соблюдать все требования, изложенные в данном документе.

Я осознаю, что нарушение данной Политики может повлечь за собой дисциплинарные, административные и/или уголовные последствия в соответствии с законодательством Российской Федерации и внутренними нормативными актами компании.

Дата: [Дата]

Подпись: _____

Расшифровка подписи: [ФИО сотрудника]

Больше интересного в нашем блоге

развивайте бизнес-мышление с нашими исследованиями



Получить пользу

