Политика безопасности

Настоящая Политика описывает основные меры безопасности, применяемые для защиты сайта HARVEY Camp, заявок пользователей и персональных данных.

Редакция от 19 июня 2026 г.

1. Назначение документа

1.1. Политика безопасности определяет общий подход Оператора к защите персональных данных и технической инфраструктуры сайта https://harvey-camp.ru/.

1.2. Оператор: БРЫНЦЕВ Тимур Романович.

1.3. Политика применяется к Сайту, форме заявки, электронной почте, материалам бронирования и техническим средствам, используемым для обработки обращений пользователей.

2. Основные принципы безопасности

Оператор придерживается следующих принципов:

- минимизация собираемых данных;
- доступ к данным только при необходимости;
- хранение данных не дольше необходимого срока;
- использование защищённых каналов связи, где это технически возможно;
- регулярная проверка актуальности контактов, форм и используемых сервисов;
- удаление устаревших заявок и лишних копий данных.

3. Технические меры защиты

3.1. Защищённое соединение

- Сайт должен работать по протоколу HTTPS.
- Передача заявок через форму должна выполняться по защищённому соединению.
- При наличии доступа к административной панели используются пароли достаточной сложности.

3.2. Контроль доступа

- Доступ к заявкам и переписке имеют только уполномоченные лица.
- Доступ к почтовым ящикам защищается паролем; при возможности используется двухфакторная аутентификация.
- Данные заявок не публикуются в открытом доступе и не передаются третьим лицам без законного основания.

3.3. Защита сайта

- Используемые CMS, плагины, скрипты и серверное ПО должны поддерживаться в актуальном состоянии.
- Неиспользуемые формы, плагины и административные учётные записи должны удаляться или отключаться.

- Форма заявки должна содержать защиту от спама и автоматизированных злоупотреблений, если это необходимо.

3.4. Резервные копии

- Резервные копии сайта и настроек могут создаваться для восстановления после технических сбоев.
- Доступ к резервным копиям ограничивается.
- Устаревшие копии, содержащие персональные данные, подлежат удалению по истечении срока хранения.

4. Организационные меры

4.1. Ответственным за организацию обработки и защиты персональных данных является Оператор лично — БРЫНЦЕВ Тимур Романович.

4.2. Оператор контролирует, какие сервисы используются для сайта, почты, форм, бронирований и оплаты.

4.3. При подключении нового сервиса Оператор оценивает, получает ли такой сервис доступ к персональным данным, и при необходимости обновляет Список обработчиков персональных данных.

4.4. Персональные данные не выгружаются и не передаются в личные устройства или сторонние сервисы без необходимости.

5. Реагирование на инциденты

5.1. Инцидентом безопасности считается неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение или иное неправомерное действие.

5.2. При обнаружении инцидента Оператор:

1. фиксирует факт инцидента и время обнаружения;
2. ограничивает дальнейший доступ к затронутым данным;
3. определяет возможный объём затронутых данных;
4. принимает меры по устранению причины инцидента;
5. при необходимости уведомляет уполномоченные органы и субъектов персональных данных в порядке, предусмотренном законом.

5.3. Если инцидент связан с обработчиком, Оператор запрашивает у обработчика сведения о причине, масштабе и принятых мерах.

6. Cookie и сторонние скрипты

6.1. Сайт может использовать технические cookies, необходимые для работы сайта и формы.

6.2. Подключение аналитических, рекламных или иных сторонних скриптов должно сопровождаться проверкой их влияния на обработку персональных данных.

6.3. Если такие скрипты собирают персональные данные или требуют согласия пользователя, Оператор размещает соответствующее уведомление и обновляет документы сайта.

7. Хранение и удаление данных

7.1. Данные заявок и переписки хранятся не дольше, чем это необходимо для обработки заявки, исполнения договора, работы с претензиями и выполнения требований закона.

7.2. Устаревшие заявки, дубликаты и лишние копии персональных данных удаляются.

7.3. По законному запросу пользователя Оператор рассматривает возможность удаления, блокирования или уточнения персональных данных.

8. Ответственное сообщение об уязвимостях

8.1. Если пользователь, исследователь безопасности или иное лицо обнаружило уязвимость на Сайте, рекомендуется сообщить об этом Оператору на email: HARVEYCamp@yandex.ru или timur301991@mail.ru.

8.2. В сообщении желательно указать адрес страницы, описание проблемы, возможные последствия и способ воспроизведения.

8.3. Оператор не разрешает проводить действия, нарушающие работу Сайта, получать доступ к чужим данным, выполнять DDoS-атаки, массовое сканирование или иные действия, нарушающие закон.

9. Связанные документы

Настоящая Политика применяется совместно со следующими документами:

- Политика обработки персональных данных;
- Публичная оферта;
- Договор-поручение на обработку персональных данных;
- Список обработчиков персональных данных.

10. Контакты

- Оператор: БРЫНЦЕВ Тимур Романович.
- Email по вопросам безопасности и персональных данных: timur301991@mail.ru.
- Email для заявок и обращений по Сайту: HARVEYCamp@yandex.ru.
- Телефон: +7 995 924-88-58.
- Сайт: https://harvey-camp.ru/.

Документ подготовлен для сайта https://harvey-camp.ru/. Перед публикацией проверьте фактические обработчики, подключённые формы, оплату, хостинг и актуальные реквизиты.