Постоянный адрес публикации документа: http://comdi.com/legal/security-policy

# ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ в ООО «ВЕБИНАР»

(выписка)

Утверждена
приказом Генерального директора
ООО «Вебинар»
(Приказ от 02.11.2021 №2021-11/21)

## ОБЩИЕ ПОЛОЖЕНИЯ

Информация является ценным и жизненно важным ресурсом Общества с ограниченной ответственностью «Вебинар» (далее – «Общество»). Настоящая Политика информационной безопасности в ООО «Вебинар» (далее – «Политика») предусматривает принятие необходимых мер в целях защиты корпоративной информации, рассматриваемой далее как ценный актив Общества от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Обществе.

Требования настоящей Политики распространяются на всех Работников Общества, а также учитываются в отношениях с Третьими лицами (контрагентами Общества).

## ЦЕЛИ

Настоящая Политика является основополагающим документом, определяющим систему приоритетов, принципов и методов обеспечения защищенности электронных Информационных ресурсов Общества. Положения Политики должны являться методологической основой для разработки нормативных и организационно-распорядительных документов Общества в области защиты информации.

Целями настоящей Политики являются:

- сохранение конфиденциальности Информационных ресурсов, используемых Обществом;
- обеспечение непрерывности доступа к информационным ресурсам Общества для поддержки бизнес-деятельности;
- защита целостности корпоративной информации с целью поддержания возможности Общества по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомлённости Работников в области рисков безопасности, связанных с информационными ресурсами Общества;
- определение степени ответственности и обязанностей Работников по обеспечению Информационной безопасности в Обществе;
- обеспечение защищённости и непрерывности бизнес-процессов;
- сохранение и защита клиентских данных;
- сохранение и защита корпоративных данных.

## ОБЛАСТЬ ПРИМЕНЕНИЯ НАСТОЯЩЕЙ ПОЛИТИКИ

Требования настоящей Политики распространяются на всю Информацию и Информационные системы Общества. Соблюдение настоящей Политики обязательно для всех Работников (как постоянных, так и временных). В договорах с Третьими лицами, получающими доступ к Информационным ресурсам Общества, должна быть оговорена обязанность Третьего лица по соблюдению требований настоящей Политики.

## СТРУКТУРА ЧАСТНЫХ ПОЛИТИК И ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Настоящая Политика, являясь документом верхнего уровня, описывает цели и основные направления их достижения.
Детальные требования различных областей информационной безопасности приведены в частных Политиках ИБ, Положении о коммерческой тайне (конфиденциальной информации) ООО «Вебинар» и режиме ее обеспечения, Положении об обработке и защите персональных данных ООО «Вебинар», инструкциях, включая, но не ограничиваясь:

- Инструкции по осуществлению парольной защиты;
- Регламенте обнаружения и реагирования на инциденты ИБ;
- Инструкции по осуществлению антивирусного контроля.

Для отдельных областей и систем допускается иметь отдельные частные политики, устанавливающие более жесткие требования и правила. В случае наличия такой политики необходимо руководствоваться ее положениями.

## ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ

В Обществе разрабатывается и поддерживается управляемый и документированный процесс обеспечения непрерывности бизнеса, учитывающий требования по Информационной безопасности. Планы непрерывности бизнеса определяют общую систему мер, ответственность, необходимые требования и условия для предотвращения прерываний критически важных бизнес-процессов, обеспечения требуемого уровня доступности Информационных ресурсов, сервисов и инфраструктуры, а также восстановления после аварии.

При организации доступа Третьим лицам к защищаемым Информационным системам в Обществе уполномоченным Руководством Общества Работником по ИБ осуществляются мероприятия по обеспечению ИБ:

- определение рисков, связанных с предоставлением доступа Третьим лицам к Конфиденциальной информации;

- формирование на основе оценки рисков перечня мероприятий по обеспечению ИБ при предоставлении доступа Третьим лицам к Конфиденциальной информации Общества и их реализация;

- заключение соглашения о конфиденциальности с Третьими лицами, которым предоставляется доступ к Конфиденциальной информации Общества.

Работники и Третьи лица, имеющие право удалённого доступа к Информационным ресурсам Общества, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Общества и к каким-либо другим сетям, не принадлежащим Обществу.

Все компьютеры, подключаемые посредством удалённого доступа к информационной сети Общества, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

Компьютерное оборудование, предоставленное Обществом, является его собственностью и предназначено для использования исключительно в служебных целях.

Все программное обеспечение, установленное на предоставленном Обществом Компьютерном оборудовании, является собственностью Общества и должно использоваться исключительно в служебных целях.

Все операционные процедуры и процедуры внесения изменений в Информационные системы и сервисы должны быть документированы, и производиться в соответствии с процедурами, согласованными с уполномоченным Руководством Общества Работником по ИБ.

Об известных или подозреваемых нарушениях Информационной безопасности Третьим лицам необходимо сообщать по адресу электронной почты security@comdi.com, а также Третьи лица должны знать о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

## ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОЛИТИКИ

Руководство Общества отвечает за состояние ИБ Общества и обеспечивает реализацию Политики, включая регулярный контроль ее исполнения, актуализацию и выделение необходимых для обеспечения ИБ ресурсов, а также организацию осведомленности и обучения Работников в области обеспечения ИБ.

Работники Общества несут ответственность за разглашение и утрату информации, подлежащей защите, а также за нарушение установленного порядка обеспечения ИБ.

Работники, разгласившие подлежащую защите информацию или нарушившие установленный порядок обращения с ней, а также Работники, по вине которых произошла ее утрата или искажение, несут ответственность в соответствии с законодательством Российской Федерации.

Работникам Общества запрещается нарушать установленные правила обеспечения ИБ и скрывать факты возникновения инцидентов ИБ.

Работники Общества, не выполняющие требования настоящей Политики и локальных нормативных актов Общества в области ИБ, могут быть привлечены к ответственности установленным порядком.