

Положение

о порядке использования информационных систем и технических средств при обработке персональных данных

1. Общие положения

1.1. Настоящее Положение определяет правила и порядок использования информационных систем, программного обеспечения, технических средств и каналов связи, применяемых в ООО «АРСАВИС», при обработке персональных данных.

1.2. Целью настоящего Положения является обеспечение безопасности персональных данных, соблюдение законодательства Российской Федерации в области обработки и защиты ПДн, а также ограничение несанкционированного доступа к информации.

1.3. Положение разработано в соответствии с Федеральным законом № 152-ФЗ «О персональных данных», а также иными нормативно-правовыми актами, регулирующими порядок обработки и защиты персональных данных.

2. Основные термины и сокращения

- ПДн — персональные данные;
- ИС — информационные системы;
- ТС — технические средства;
- Сотрудник — любое лицо, работающее с ПДн в интересах ООО «АРСАВИС».

3. Порядок использования информационных систем и технических средств

3.1. Обработка ПДн осуществляется с использованием технических средств и ИС, принадлежащих ООО «АРСАВИС», либо переданных в её пользование по договору.

3.2. Использование технических средств (компьютеров, телефонов, планшетов и пр.) допускается исключительно в служебных целях.

3.3. Установка и использование стороннего программного обеспечения без согласования с ответственным за информационную безопасность не допускается.

3.4. Запрещено использование личных USB-носителей и внешних дисков без предварительного сканирования антивирусным ПО.

3.5. Запрещено передавать логины и пароли третьим лицам, включая других сотрудников, за исключением прямого распоряжения руководства.

3.6. Доступ к ИС, содержащим ПДн, предоставляется строго в рамках служебной необходимости.

4. Требования к защите информации

4.1. Сотрудники обязаны:

- использовать сложные пароли для входа в системы и регулярно их менять;
- блокировать рабочее место при уходе от компьютера;
- немедленно сообщать ответственному лицу об инцидентах информационной безопасности.

4.2. Все передаваемые по сети персональные данные должны быть защищены с использованием криптографических (шифровальных) средств, сертифицированных ФСТЭК/ФСБ.

5. Ответственность

5.1. За нарушение настоящего Положения сотрудники несут дисциплинарную, административную и иную ответственность в соответствии с действующим законодательством РФ и локальными нормативными актами организации.

5.2. Обязательно ознакомление сотрудников с настоящим Положением.

6. Заключительные положения

6.1. Настоящее Положение вступает в силу с даты утверждения и подлежит обязательному пересмотру не реже одного раза в 3 (три) года либо при изменении нормативно-правовой базы.

6.2. Настоящее Положение является обязательным для исполнения всеми сотрудниками, имеющими доступ к ПДн и техническим средствам.

Памятка для сотрудников
«Как безопасно использовать рабочие устройства
при работе с персональными данными»

Уважаемые коллеги!

Во избежание утечек персональных данных и нарушений закона, придерживайтесь следующих правил:

1. **Не используйте рабочий компьютер в личных целях**, не устанавливайте стороннее ПО без согласования.
2. **Всегда блокируйте экран**, если отходите от рабочего места.
3. **Храните персональные данные только в защищённых папках** (с ограничением доступа).
4. **Передавайте ПДн только через защищённые каналы** — почта с шифрованием, внутренние системы.
5. **Никому не передавайте свои логины и пароли.**
6. **Не используйте личные флешки и внешние устройства без согласования с ответственным.**
7. **Соблюдайте правила работы в системе**, изложенные в Положении и других локальных актах.
8. **Немедленно сообщайте** о любых сбоях, подозрениях на вирус или утечку данных ответственному лицу.

Нарушения могут повлечь **ответственность вплоть до увольнения и штрафов для компании.**

Сохраняйте бдительность —

вы отвечаете за безопасность информации не меньше, чем за рабочие задачи!