АССОЦИАЦИЯ СТРОИТЕЛИ ОМСКА

644043, г. Омск,
ул. Красный Путь, 101, пом 72П/5
тел. +7(900)672-99-33

ИНН 5503173432 ОГРН 1175543011731
сайт: строителиомска.рфe-mail: stroiteliomska@yandex.ru

ПРИКАЗ № ПД-1

г. Омск «20 » июня 2019 года

«Об утверждении Положения об обработке и обеспечении безопасности персональных данных в Ассоциации «Строители Омска»

Во исполнение требований Федерального закона от 27.07.2006 год № 152-ФЗ

1. Утверждаю Положение об обработке и обеспечении безопасности персональных данных в Ассоциации «Строители Омска» с приложениями.
2. Юрисконсульту Ассоциации Поповой В.В. ознакомить всех сотрудников с Положением, указанным в пункте 1 настоящего приказа, включая Приложения к нему, обеспечить размещение указанного в пункте 1 настоящего Приказа Положения, включая Приложения к нему на официальном сайте в сети Интернет.
3.

Генеральный директор О.Б. Козубович

С Приказом ознакомлены:

1. Попова Виктория Васильевна 20.06.2019
2. Бочкарев Владимир Григорьевич 20.06.2019
3. Выгодская Анна Геннадьевна 20.06.2019г
4. Бессольцев Георгий Олегович 20.06.2019г
5. Ким Наталья Николаевна 20.06.2019г
6. Бондарев Олег Игоревич 20.06.2019г.
7. Ляшенко Антон Николаевич 20.06.2019
8. Сковородова Светлана Александровна 15.10.2019
9. Рубан Павел Александрович 29.09.2020

Утверждено
Приказом
генерального директора
№ПО-1 от 20.06.19 года

Положение об обработке и обеспечению безопасности персональных данных в Ассоциации «Строители Омска»

I. Общие положения.

1. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3. Ассоциация «Строители Омска» (далее–Ассоциация, Оператор) обеспечивает безопасность персональных данных при их обработке в информационной системе.

4. Выбор средств защиты информации для системы защиты персональных данных осуществлён в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

5. Обработка персональных данных осуществляется в порядке, определённом политикой Ассоциации «Строители Омска» в отношении обработки персональных данных, утверждённой генеральным директором Ассоциации «Строители Омска» 22.12.2017 года, а в части неурегулированной Политикой – настоящим Положением.

II. Определение типа угроз и необходимого уровня защищённости персональных данных.

Информационная система является информационной системой персональных данных субъектов персональных данных, не являющихся сотрудниками Оператора.

1. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

2. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, произведено с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

- Разряд персональных данных, обрабатываемых в информационной системе Ассоциации – иные;
- Количество персональных данных – менее 100 000;
- Для информационной системы актуальны угрозы, несвязанные с недокументированными (недекларированными) возможностями в системном и прикладном программном обеспечении.
- строение информационной системы – локальное;
- подключения информационной системы к сетям публичного применения – отсутствует;
- режим обработки персональных данных – с наличием границ доступа;
- при обработке персональных данных в информационных системах установлен 4 уровень защищенности персональных данных.
- необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе установлена по наличию следующего условия: для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

3. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах выполняются следующие требования:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем Оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

4. Контроль за выполнением настоящего Положения организуется и проводится Ассоциацией самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые Ассоциацией.

III. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации.

1.Организация режима обеспечения безопасности помещений, в которых размещена информационная система персональных данных препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

1.1 Помещения оборудованы входными дверьми с замками в количестве - 3 двери, обеспечено постоянное закрытие 1 двери помещений на замок и их открытия только для санкционированного прохода, а также оборудование помещений техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

1.2 Утверждены правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях.

1.3. Утверждён переченьлиц, имеющих право доступа в Помещения.

2. Обеспечение сохранности носителей персональных данных.

2.1. Хранение съемных машинных носителей персональных данных осуществляется в сейфах (металлических шкафах), оборудованных внутренними замками с двумя дубликатами ключей и приспособлениями для опечатывания замочных скважин. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, хранение таких носителей осуществляется вне сейфов (металлических шкафов).

2.2. Осуществление поэкземплярного учет машинных носителей персональных данных, путем ведения журнала учета машинных носителей персональных данных с использованием регистрационных (заводских) номеров.

3. Утверждение руководителем Оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей и назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

3.1. Разработан и утверждён документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

3.2. Поддержание в актуальном состоянии документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей, достигается контролем и внесением в него изменений по мере внесения изменений в должностные обязанности и при приёме на работу, увольнении с работы, переводах и прочих кадровых изменениях.

3.3. Назначено обладающее достаточными навыками лицо (работник), ответственное за обеспечение безопасности персональных данных в информационной системе (для третьего уровня).

4. Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз(подлежит применению после принятия Технического регламента процедуры оценки соответствия, в порядке Федерального закона от 27.12.2002 № 184-ФЗ

(ред. от 28.11.2018) «О техническом регулировании»).

4.1 . Получение исходных данных для формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

4.2. Формирование и утверждение руководителем Оператора совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ;

4.3. Использование для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше.

IV. Состав и содержание мер по обеспечению безопасности персональных данных

1. В состав мер по обеспечению безопасности персональных данных, реализуемых Ассоциацией в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа, которыми обеспечено присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности);

- управление доступом субъектов доступа к объектам доступа, которыми обеспечено управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа (должностных обязанностей), а также обеспечение контроля за соблюдением этих правил;

- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных), которыми исключена возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных;

- регистрация событий безопасности, которой обеспечены сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них;

- антивирусная защита, которой обеспечено обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;

- контроль (анализ) защищенности персональных данных, которыми обеспечены контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

- защита среды виртуализации, которой исключен несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействию на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям;

- защита технических средств, которой исключен несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

- защита информационной системы, ее средств, систем связи и передачи данных, которой обеспечено защита персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

2. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в

информационной системе в рамках системы защиты персональных данных, определён базовым набором мер по обеспечению безопасности персональных данных для установленного четвёртого уровня защищенности персональных данных в соответствии Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Базовый набор мер адаптирован с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе) Ассоциации;

3. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

V. Состав и содержание мер по обеспечению безопасности персональных данных.

1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками Оператора

ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

ИАФ.5 Защита обратной связи при вводе аутентификационной информации

ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками Оператора (внешних пользователей)

2. Управление доступом субъектов доступа к объектам доступа (УПД)

УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей

УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа

УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы

УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы

УПД.6 Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)

УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети + +

УПД.14 Регламентация и контроль использования в информационной системе технологий беспроводного доступа

УПД.15 Регламентация и контроль использования в информационной системе мобильных технических средств

УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

3. Защита машинных носителей персональных данных (ЗНИ)

ЗНИ.8 Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их

передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания

4. Регистрация событий безопасности (РСБ)

РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения

РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

РСБ.7 Защита информации о событиях безопасности + +

5. Антивирусная защита (АВЗ)

АВЗ.1 Реализация антивирусной защиты

АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

6. Контроль (анализ) защищенности персональных данных (АНЗ)

АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

АНЗ.4 Контроль состава технических средств, программного обеспечения и средств защиты информации

7. Защита среды виртуализации (ЗСВ)

ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации

ЗСВ.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин

8. Защита технических средств (ЗТС)

ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены

ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

Приложения:

1) Правила доступа работников Ассоциации «Строители Омска», в которых ведется обработка персональных данных;
2) Типовая форма журнала учета машинных носителей персональных данных.
3) Типовая форма журнала учёта съёмных носителей персональных данных.
4) Порядок по учету и хранению съёмных носителей персональных данных
5) Типовое согласие на обработку персональных данных работника;
6) Типовое обязательство о неразглашении персональных данных.
7) Акт классификации информационных систем персональных данных используемых в Ассоциации «Строители Омска» при обработке персональных данных
8) Инструкция по регистрации событиями информационной безопасности
9) План внутренних проверок состояния защиты персональных данных
10) Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
11) Правила и процедуры идентификации и аутентификации субъектов доступа к объектам доступа
12) Правила рассмотрения запросов субъектов персональных данных или их представителей в Ассоциации «Строители Омска»
13) Типовая форма согласия на обработку персональных данных сотрудников организаций и ИП – членов СРО Ассоциации «Строители Омска».
14) Типовая форма согласия на обработку персональных данных для внесения в НРС

Приложение № 1
к положению об обработке и обеспечению
безопасности персональных данных
в Ассоциации «Строители Омска»

Правила доступа работников Ассоциации «Строители Омска»
в помещения, в которых ведется обработка персональных данных

1. Общие положения.

1.1 Настоящий Порядок определяет процедуру доступа работников Ассоциации «Строители Омска» (далее – Ассоциация) в помещения, в которых ведется обработка персональных данных и разработан в соответствии с Приказом ФСБ РФ от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Целью настоящего Порядка является обеспечение исключения неправомерного или случайного доступа к материальным носителям персональных данных и техническим средствам их обработки, а также иных неправомерных действий в отношении персональных данных.

2. Порядок доступа в помещения, в которых ведется обработка персональных данных.

2.1. Доступ работников Ассоциации, в помещения, в которых ведется обработка персональных данных, осуществляется согласно перечню должностей Ассоциации, допущенных к обработке персональных данных, утвержденному приказом генерального директора, в рабочее время,

2.2. Пребывание посторонних лиц в кабинетах, в которых ведется обработка персональных данных, допускается только в присутствии работников Ассоциации, допущенных в помещения, в которых ведется обработка персональных данных.

2.3. Работники сторонних организаций, прибывшие в помещения, в которых ведется обработка персональных данных, для выполнения работ, оказания услуг в соответствии с заключенными Ассоциацией контрактами (договорами), допускаются в помещение только в присутствии работников Ассоциации, при проведении таких работ, работники Ассоциации обязаны принять меры по исключению ознакомления работников сторонних организаций с персональными данными.

3. Порядок вскрытия и сдачи под охрану помещений, в которых ведется обработка персональных данных.

3.1. Помещения, в которых ведется обработка персональных данных, по окончании рабочего дня должны закрываться на ключ, а офис Ассоциации передается под охрану. В Ассоциации установлена охранная сигнализация.

3.2. Для входа в офис Ассоциации все сотрудники имеют идентификационные пароли для снятия охранной сигнализации. Вскрытие и закрытие помещения осуществляют сотрудники Ассоциации, допущенные в данное помещение.

3.3. При завершении рабочего дня сотрудники отделов обязаны выполнить следующие мероприятия:

- убрать документы с персональными данными в шкафы, сейфы или запирающиеся на ключ шкафы;
- выключить установленным порядком вычислительную технику и оргтехнику;
- закрыть окна;
- выключить электроприборы;
- выключить свет;
- закрыть входную дверь на замок;
- установить охранную сигнализацию;
- ключ от входной двери в помещение сотрудник отделения сохраняет у себя.

3.4. Сотрудники, вскрывающие помещение, в котором ведется обработка персональных данных, обязаны выполнить следующие мероприятия:

- проверить целостность входной двери помещения;
- вскрыть помещение;
- проверить целостность сейфа (шкафа, тумбочек), наличие и целостность компьютерной и оргтехники;
- при обнаружении нарушения целостности двери, сейфа, шкафа, тумбочек, отсутствии или нарушении целостности вычислительной техники, других нарушениях сотрудник, вскрывающий помещение, в котором ведется обработка персональных данных, обязан прекратить вскрытие помещения, доложить о выявленных нарушениях своему непосредственному руководителю.

3.5. В нерабочее время работники Ассоциации имеют доступ в помещения по предварительному разрешению Руководителя Ассоциации. Посторонние лица в нерабочее время в помещение не допускаются. Руководитель Ассоциации имеет право доступа в помещение в любое время.

3.6. Нештатные ситуации это затопление, пожар, срабатывание тревожной сигнализации, иные события, обстоятельства, требующие незамедлительного доступа в помещение. При возникновении нештатной ситуации работник, которому стало об этом известно, незамедлительно должен сообщить руководителю о возникновении нештатной ситуации. Сотрудники органов МЧС, аварийных служб, врачи скорой помощи допускаются в помещение в сопровождении руководителя Ассоциации или лица, которому руководитель поручил обеспечить сопровождение указанных служб.

4. Запрещается

4.1. Запрещается оставлять помещения, в которых ведется обработка персональных данных, без присмотра работников, имеющих допуск в помещения, где ведется обработка персональных данных.

4.2. Запрещается оставлять без присмотра находящихся в помещении, в которых ведется обработка персональных данных, посторонних лиц, а также работников, не имеющих допуск в помещения, в которых ведется обработка персональных данных.

5. Внутренний контроль

5.1. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, осуществляется лицом, ответственным за обработку персональных данных.

6. Ответственность

6.1. Работники, нарушившие нормы настоящего Порядка, несут ответственность в соответствии с действующим законодательством.

Утверждено Приказом №1102 от 20.06.2019г

Журнал учета машинных носителей персональных данных

Начат «_____» _____ 20__ года на _____ листах

Окончен «_____» _____ 20__ года

_____

_____ _____

Должность, Ф.И.О., ответственного за хранение Подпись

№ п/п	Регистрационный номер/дата	Тип/ёмкость машинного носителя персональных данных	Номер экземпляра/ количество экземпляров	Место установки (использования)/ дата установки	Ответственное должностное лицо , Пользователь (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)
1									
2									
3									
4									
5									

Утверждено Приказом №102 от 10.08.2019

Журнал учета съемных носителей персональных данных

Начат «_____» _____ 20__ года на _____ листах

Окончен «_____» _____ 20____ года

_____ _____

Должность, Ф.И.О., ответственного за хранение Подпись

№ п/п	Регистрационный номер/дата	Тип/ёмкость съёмного носителя персональных данных	Номер экземпляра/ количество экземпляров	Место использования	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения съёмного носителя персональных данных	Сведения об уничтожении съёмного носителя персональных данных, стирании информации (подпись, дата)
1									
2									
3									
4									
5									

Приложение № 4
к положению об обработке и
обеспечению
безопасности персональных
данных
в Ассоциации «Строители Омска»

Порядок
по учету и хранению носителей персональных данных

1. С настоящим Порядком знакомятся под подпись и выполняют его все сотрудники Ассоциации «Строители Омска» (далее – Ассоциация), допущенные к обработке персональных данных.

2. Порядок использования носителей информации

2.1. Под использованием носителей информации в информационной системе понимается их подключение к инфраструктуре информационной системы с целью обработки, приема/передачи информации между информационной системой и носителями информации.

2.2. В информационной системе допускается использование только учтенных носителей информации, которые являются собственностью Ассоциации и подвергаются регулярной ревизии и контролю.

Учету подлежат:

- съемные машинные носители персональных данных (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

- портативные вычислительные устройства, имеющие встроенные носители персональных данных (ноутбуки, сотовые телефоны, цифровые камеры и инфе по функциональности устройства);

-машинные носители персональных данных, встроенные в корпус средства вычислительной техники (накопители на жестких дисках)

2.3. Для учета носителей персональных данных проводится обязательное присвоение регистрационных учетных номеров. В качестве регистрационных номеров могут использоваться серийные номера машинных носителей.

2.4. Учет машинных носителей персональных данных ведется в журнале учета машинных носителей персональных данных.

2.5. Регистрационные номера вносятся в журнал учета машинных носителей персональных данных с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям персональных данных.

3. Порядок учета, хранения и обращения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации.

3.1. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в Ассоциации подлежат учёту.

3.2. Каждый съемный носитель с записанными на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

3.3. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляет уполномоченный сотрудник, отвечающий за хранение информации. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

3.4. Сотрудники Ассоциации получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

4. При использовании сотрудниками носителей конфиденциальной информации необходимо:

4.1. Соблюдать требования настоящего Положения.

4.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.

4.3. Обеспечивать физическую безопасность носителей информации всеми разумными способами.

4.4. Извещать администраторов информационной системы о фактах утраты (кражи) носителей конфиденциальной информации.

5. Организация хранения съемных носителей персональных данных.

5.1. Хранение носителей осуществляется в условиях, исключающих несанкционированное копирование, изменение или уничтожение информации ограниченного доступа, а также хищение носителей. Носители должны храниться в служебных помещениях, в металлическом шкафу (сейфе).

5.2. Запрещается хранить съемные носители персональных данных вместе с носителями открытой информации, на рабочих столах, оставлять их без присмотра или передавать на хранение другим лицам, выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, а также использовать носители персональных данных в личных целях.

5.3. В случае утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений, ставится в известность ответственное лицо за организацию обработки персональных данных в Ассоциации. Соответствующие отметки вносятся в журнал учета съемных носителей, содержащих персональные данные.

5.4. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с персональными данными осуществляется комиссией Ассоциации. По результатам уничтожения носителей составляется акт уничтожения съемных носителей персональных данных (Приложение №1 к настоящему Порядку).

6. Организация контроля за работой со съемными носителями персональных данных.

6.1. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником Ассоциации между информационной системой и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администраторами ИС заранее). Администратор информационной системы оставляет за собой право блокировать или ограничивать использование носителей информации.

6.2. Информация, хранящаяся на носителях конфиденциальной информации, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.

6.3. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

6.4. Вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

6.5. В случае увольнения работника предоставленные носители конфиденциальной информации изымаются.

7. Ответственность

7.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами органа исполнительной власти.

Приложение № 1
к Порядку
по учету и хранению носителей
персональных данных

"УТВЕРЖДАЮ"

_____

"____ "_____ 20__ г.

АКТ
уничтожения съемных носителей персональных данных

Комиссия в составе:

_____

_____

_____

_____

_____

провела отбор съемных носителей персональных данных, не подлежащих дальнейшему использованию (хранению):

№ п/п	Дата регистрации	Учетный номер съемного носителя	Примечание

Всего съемных носителей _____
(цифрами и прописью)

На съемных носителях уничтожены персональные данные путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены путем

_____
(разрезания, демонтажа, сжигания, крошения и т.п.)

Председатель комиссии _____

Члены комиссии _____

_____

Приложение № 5
к положению об обработке и обеспечению
безопасности персональных данных
в Ассоциации «Строители Омска»

_____
(фамилия, имя, отчество)
_____
(адрес регистрации с почтовым индексом)
_____
(паспортные данные, орган выдавший паспорт)
_____
(мобильный телефон)

СОГЛАСИЕ
на обработку персональных данных

Я, _____, в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в целях:
- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними;
- отражения информации в кадровых документах;
- начисления заработной платы;
- исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ;
- предоставления сведений в кредитную организацию для оформления банковской карты иперечисления на нее заработной платы;
- предоставления сведений третьим лицам для оформления полиса ДМС;
- предоставления налоговых вычетов;
- обеспечения моей безопасности;
- контроля количества и качества выполняемой мной работы;
- обеспечения сохранности имущества работодателя

даю согласие

Ассоциации «Строители Омска» (ИНН 5503173432 ОГРН 1175543011731), на автоматизированную, а также без использования средств автоматизации, обработку моих персональных данных, а именно на сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Перечень моих персональных данных, на обработку которых я даю согласие:
- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона (домашний, мобильный};
- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;
- семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством;
- отношение к воинской обязанности;
- сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;

- СНИЛС;
- ИНН;
- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в Ассоциации «Строители Омска»;
- сведения о доходах в Ассоциации «Строители Омска»;
- сведения о деловых и иных личных качествах, носящих оценочный характер.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

Дата заполнения «___»_____ 20___ г.

_____

(подпись) (Ф.И.О. работника, дающего согласие на обработку персональных данных)

Приложение № 6
к положению об обработке и обеспечению
безопасности персональных данных
в Ассоциации «Строители Омска»

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО

работника Ассоциации «Строители Омска», непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я, _____
(фамилия, имя, отчество)

_____
(должность)

_____

обязуюсь в случае расторжения трудового договора, заключенного между мной и Ассоциацией «Строители Омска», прекратить обработку персональных данных, ставших мне известными в связис исполнением должностных обязанностей.

В соответствии со статьей 7 Федерального законаот 27.07.2006 № 152-ФЗ«О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальнойинформацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшихизвестными мне в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная Федеральным законом от 27.07.2006 № 152-ФЗ «О персональныхданных» и другими Федеральными законами, мне разъяснена.

«____» _____ 20____ г. _____ _____
(дата) (подпись) (расшифровка подписи)

Приложение № 7
к положению об обработке и обеспечению
безопасности персональных данных
в Ассоциации «Строители Омска»

АКТ
классификации информационных систем персональных данных, используемых в Ассоциации «Строители Омска» при обработке персональных данных

В соответствии с Постановлением Правительства Российской Федерации от 01.11.2012. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом Генерального директора Ассоциации «Строители Омска» от «13» мая 2019 № ____ комиссия в составе:

председатель комиссии: Болдырев О.И.

члены комиссии: Ляшенко О.Н., Клим Н.Н., Попова В.В.

с целью самостоятельной экспертной оценки уровня защищенности персональных данных, обрабатываемых в информационных системах Ассоциации «Строители Омска» (далее - Ассоциация) произвела сбор и анализ данных об информационных системах используемых для обработки персональных данных и установила нижеследующее:

1. Категорий персональных данных, обрабатываемых в информационных системах Ассоциации - ***иные***;
2. В информационных системах Ассоциации одновременно обрабатываются персональные данные ***менее чем 100 000 субъектов персональных данных***;
3. По структуре в информационных системах Ассоциации относится к ***локальной информационной системе***, состоящей из нескольких автоматизированных рабочих мест;
4. По наличию подключений к сетям международного информационного обмена (Интернет) информационная система относится к системам, ***не имеющим подключения***;
5. По режиму обработки персональных данных информационные системы Ассоциации относятся к:

- информационная система 1-С Бухгалтерия – однопользовательская;
- информационная система НСР – однопользовательская;
- информационная система реестр членов СРО – однопользовательская;
- информационная система База СРО (внутренняя) – многопользовательская.

6. По разграничению прав доступа пользователей информационной системы относится к системам с ***разграничением прав доступа;***

7. В зависимости от местонахождения технических средств в информационных системах Ассоциации относится к системам, технические средства которых размещены в Российской Федерации;

8. Речевая обработка сведений составляющих в информационных системах Ассоциации в информационной системе ***не осуществляется***.

9. Условие обработки персональных данных — для информационной системы актуальны ***угрозы 3-го типа*** и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора.

В соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и на основании анализа исходных данных информационной системе персональных данных в информационных системах Ассоциации установить ***уровень защищенности 4***.

Председатель комиссии: _____ / О.И. Бондарев /
«20» 06 2019 г.

Члены комиссии:
1. _____ / В.В. Попова
2. _____ / А.Н. Мясников
3. _____ / О.И. Бондарев /
4. _____ / И.Н. Ильин /

Приложение № 8
к положению об обработке и обеспечению
безопасности персональных данных
в Ассоциации «Строители Омска»

ИНСТРУКЦИЯ
по регистрации событий информационной безопасности

Настоящая инструкция определяет для информационной системы (далее – ИС) Ассоциации «Строители Омска»:

1. Перечень событий информационной безопасности (далее – событий ИБ), подлежащих регистрации и сроки их хранения.

2. Состав и содержание информации о событиях безопасности, подлежащих регистрации.

3. Порядок сбора, записи и хранения информации о событиях безопасности в течение определенного времени хранения.

4. Порядок защиты информации о событиях безопасности.

1. Регистрация событий ИБ

1.1. В регистрируемые события ИБ должны быть включены события ИБ, имеющие отношение к возможности реализации угроз безопасности информации, обрабатываемой в ИС, описанных в модели угроз безопасности информации для ИС.

1.2. К регистрируемым событиям ИБ относятся события безопасности, регистрируемые в журналах операционных систем технических средств ИС и средств защиты информации (далее – СЗИ), а также организационно-технические события информационной безопасности в инфраструктуре ИС.

1.3. Автоматически определяемые события ИБ регистрируются автоматически в электронных журналах сообщений программных средств ИС и средств защиты информации (СЗИ).

1.4. События ИБ, не определяемые автоматически, регистрируются в журнале событий безопасности по форме Приложения №1 к настоящей Инструкции.

1.5. Перечень событий безопасности, не определяемых автоматически, которые необходимо регистрировать при их возникновении, приведен в перечне регистрируемых событий ИБ (Приложение №2 к настоящей Инструкции).

2. Порядок сбора, записи и хранения событий ИБ

2.1. Настройку журналов регистрации событий ИБ в программном обеспечении ИС и СЗИ осуществляет системный администратор ИС на основании предоставленных полномочий. Настройка осуществляется в соответствии с эксплуатационной документацией на программно – технические средства ИС.

2.2. Системный администратор ИС должен с периодичностью не реже 1 раза в неделю просматривать журналы регистрации событий безопасности ИС.

2.3. Настройки журналов регистрации событий информационной безопасности должны обеспечивать запись в память технических средств ИС и СЗИ информации о поступающих событиях безопасности без переполнения памяти в течение 1 месяца с момента регистрации события.

2.4. Информация о событиях безопасности в ИС, не подлежащая автоматической регистрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового плана), должна фиксироваться системным администратором при ее обнаружении в журнале событий безопасности.

3. Защита информации о событиях ИБ

3.1. Права доступа к файлам отчетов электронных журналов безопасности и настройкам журналов установлены системному администратору ИС.

3.2. Доступ к электронным журналам безопасности должен быть блокирован при пользовательском уровне доступа к ИС.

3.3. Ответственность за сохранность журнала событий безопасности по форме Приложения №1 и за конфиденциальность заносимой в него информации несет системный администратор.

4. Заключительные положения

4.1. Сотрудники Организации, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

5. Нормативные и правовые документы

5.1. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5.2. Приказ ФСТЭК России от 23.03.2017 № 49 «О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21, и в требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31».

5.3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Генеральный директор О.Б. Козубович

Приложение № 1

к Инструкции по управлению
событиями информационной безопасности

ЖУРНАЛ
событий информационной безопасности.

Начат: «___» _____ 20____ г.

Окончен: «___» _____ 20____ г.

1	2	3	4	5	6
№	Код события (в соответствии с перечнем регистрируемых событий ИБ)	Место события	Участники события	Дата	Подпись системного администратора

ПРАВИЛА

по формированию и ведению журнала событий информационной безопасности

ФОРМИРОВАНИЕ ЖУРНАЛА.

Журнал формируется из стандартных листов формата А4 в альбомной ориентации.

Обложка журнала изготавливается на отдельном листе.

Все листы журнала, за исключением листов обложки, нумеруются.

Все листы журнала вместе с обложкой сшиваются.

ВЕДЕНИЕ ЖУРНАЛА.

Графы журнала заполняются следующим образом:

Графа 1 – порядковый номер записи.

Графа 2 – код события из перечня регистрируемых событий (например – пароль пользователя не соответствует требованиям – записать код 006).

Графа 3 – указывается название рабочего места пользователя (например – АРМ №3).

Графа 4 – указываются участники события (например – для кода 006 это – пользователь Иванов И.И. и системный администратор Сидоров С.С.).

Графа 5 – для несъемных носителей указывается АРМ пользователя.

Граф 6 –ФИО пользователя (например – Иванов И.И.).

Графа 7 – дата события (например – обнаружено 01.01.2017).

Графа 8 – подпись системного администратора (например – Сидоров С.С.)

Все записи в журнале делаются четко и разборчиво. В случае, если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк.

Приложение № 2
к Инструкции по управлению
событиями информационной безопасности

ПЕРЕЧЕНЬ
регистрируемых событий информационной безопасности ИС «Ассоциация «Строители Омска»

№ группы	Группа	Код события	Событие
1	Идентификация и аутентификация пользователей и устройств	001	Устаревший пароль (не соблюдены требования к срокам обновления пароля)
		002	Скомпрометированный пароль (пароль пользователя известен другому лицу)
		003	Утеря пароля (блокировка входа после неверного 3-х кратного входа)
		004	Пользователь не внесен в журнал выдачи первичных паролей
		005	Нет отметки в журнале выдачи первичных паролей отметки о блокировании доступа уволенному сотруднику.
		006	Пароль пользователя не соответствует требованиям
		007	Бездействие пользователя более установленного времени (блокировка доступа по истечению установленного интервала)
		008	Утеря аппаратного средства аутентификации.
		009	Порча аппаратного средства аутентификации
		010	
2	Машинные носители информации	011	Отсутствует учетный номер на МНИ и запись в журнале учета
		012	Превышение срока пользования учтенным МНИ
		013	Запись на учтенный МНИ иной информации вместе с обрабатываемой информацией
		014	Несанкционированный вынос МНИ из зоны обработки информации
		015	Несанкционированная передача МНИ другому пользователю
		016	Хранение МНИ на рабочем столе пользователя
		017	МНИ, оставленный без присмотра
		018	
		019	
		020	
3	Вирусы	021	Вирусная атака (заражение)
		022	Истек срок лицензии на антивирусное ПО и ПО не обновлено
		023	Сбои (нарушения в работе) антивирусного ПО

		024	
		025	
4	Контролируемая зона	026	Вынос учтенного оборудования ИС за границы контролируемой зоны
		027	Внутри контролируемой зоны неучтенные МНИ или неучтенные технические средства чтения и записи информации.
		028	Экран монитора виден со стороны двери или окон в контролируемом помещении
		029	В помещении контролируемой зоны отсутствуют сотрудник, помещение не заперто.
		030	В помещении контролируемой зоны без сопровождения присутствует сотрудник, не имеющий допуска к обработке информации.
		031	
		032	
		033	
		034	
		035	
5	СКЗИ	036	Компрометация СКЗИ (ключевая информация известна другому пользователю)
		037	Утеря СКЗИ или ключевой информации.
		038	Информация в журнале учета СКЗИ неактуальна (не обновлена)
		039	Нахождение инсталлирующих носителей, ЭД и ТД на СКЗИ в неположенном месте
		040	Действующие и резервные ключевые документы хранятся нераздельно
		041	Отсутствие или нарушение опломбирования оборудования с СКЗИ
		042	
		043	
		044	
		045	
6	ПО	046	Несанкционированная АБ установка (обновление) ПО
		047	ПО на дистрибутивных носителях не имеет лицензии.
		048	Хранение дистрибутивных носителей с устаревшим ПО
		049	Нет сведений о совместимости обновлений ПО с установленными СВТ
		050	

Приложение № 9
к положению об обработке и обеспечению
безопасности персональных данных
в Ассоциации «Строители Омска»

ПЛАН
внутренних проверок состояния защиты персональных данных

Мероприятие	Периодичность	Исполнитель
Осуществление внутреннего контроля за соблюдением сотрудниками Ассоциации законодательства РФ о персональных данных, в том числе требований к защите персональных данных	Постоянно	Начальник экспертного отдела - юрисконсульт
Доведение до сведения положения законодательства РФ о персональных данных, разработанных внутренних локальных актов по вопросам обработки персональных данных, требований к защите персональных данных	По мере необходимости	Начальник экспертного отдела - юрисконсульт
Учет всех защищаемых носителей информации с помощью их маркировки и занесение учётных данных в Журнал учёта с отметкой об их выдаче (приеме)	Ежеквартально	Главный бухгалтер
Порядок и условия хранения бумажных носителей, содержащих персональные данные	Еженедельно	Руководители отделов, комиссия по персональным данным
Соблюдение правил доступа к бумажным носителям с персональными данными	Еженедельно	Руководители отделов, комиссия по персональным данным
Соблюдение условий доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.	Еженедельно	Руководители отделов, комиссия по персональным данным
Соблюдение режима обработки персональных данных	Еженедельно	Руководители отделов, комиссия по персональным данным
Соблюдение режима защиты	Ежедневно	Системный администратор
Соблюдение требований антивирусной защиты, обновление антивирусных баз	Еженедельно	Системный администратор
Соблюдение режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Системный администратор
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты персональных данных	Ежегодно	Системный администратор , комиссия по

		персональным данным
Организация анализа и пересмотра имеющихся угроз безопасности персональных данных, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	Комиссия по персональным данным
Контроль за обеспечением резервного копирования	Ежемесячно	Системный администратор
Соблюдение правил работы со съемными носителями персональных данных	Еженедельно	Руководители подразделений, комиссия по персональным данным
Своевременность проведения мероприятий по обезличиванию персональных данных	Ежемесячно	Руководители подразделений, комиссия по персональным данным
Своевременность проведения мероприятий по уничтожению персональных данных	Ежемесячно	Руководители подразделений, комиссия по персональным данным
Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями	Ежемесячно	Комиссия по персональным данным
Своевременность и эффективность проведенных дополнительных мероприятий по обеспечению безопасности персональных данных.	Ежемесячно	Комиссия по персональным данным
Соответствие используемых Пользователями ИСПДн полномочий параметрам (матрице) доступа	Еженедельно	Руководители подразделений, комиссия по персональным данным
Организация анализа и пересмотра имеющихся угроз безопасности персональных данных, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	Комиссия по персональным данным
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	Начальник экспертного отдела – юрисконсульт
Ведение журнала внутренних проверок и поддержание его в актуальном состоянии	Ежемесячно	Комиссия по персональным данным
Установка и смета паролей доступа на персональные компьютеры	Ежеквартально	Комиссия по персональным данным

Приложение № 10
к положению об обработке и обеспечению
безопасности персональных данных
в Ассоциации «Строители Омска»

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) определяются основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным закономот 27.07.2006 № 152-ФЗ«О персональных данных» и другими нормативными правовыми актами.

2. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального законаот 27.07.2006 № 152-ФЗ«О персональных данных».

3. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - требования)в Ассоциации «Строители Омска» (далее – Ассоциация) организовывается проведение периодических проверок условий обработки персональных данных в Ассоциации.Проверки осуществляются лицом, ответственным за организацию обработки персональных данных в Ассоциации и (или) комиссией по персональным данным и (или) специально созданной комиссией.

4. В проведении проверки не может участвовать работник, прямо или косвенно заинтересованный в ее результатах.

5. Проверки проводятся на основании планов осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего оператору письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

6. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

1) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

2) порядок и условия применения средств защиты информации;

3) эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

4) состояние учета машинных носителей персональных данных;

5) соблюдение правил доступа к персональным данным;

6) наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

7) осуществление мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) осуществление мероприятий по обеспечению целостности персональных данных.

7. Лицо, ответственное за организацию обработки персональных данных в Ассоциации, комиссия имеют право:

1) запрашивать информацию, необходимую для реализации своих полномочий;

2) требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

3) принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

4) вносить оператору предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

5) вносить оператору предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

8. В отношении персональных данных, ставших известными лицу, ответственному за организацию обработки персональных данных оператора, комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

9. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о ее проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, сроках их устранения лицо, ответственное за организацию обработки персональных данных, либо председатель комиссии докладывает генеральному директоруАссоциации в форме письменного заключения.

Приложение № 11
к положению об обработке и обеспечению
безопасности персональных данных
в Ассоциации «Строители Омска»

ПРАВИЛА
и процедуры идентификации и аутентификации субъектов доступа к объектам доступа

1. Назначение и область действия документа

1.1. В настоящих Правилах и процедурах идентификации и аутентификации субъектов доступа к объектам доступа (далее – Правила) определяются правила и процедуры идентификации и аутентификации в информационных системах Ассоциации «Строители Омска» (далее Ассоциация), в которых обрабатывается информация, доступ к которой ограничен федеральными законами, включающие в себя регламентацию следующих правил и процедур:

1.1.1. Правила и процедуры идентификации и аутентификации пользователей, являющихся работниками Ассоциации;

1.1.2. Правила и процедуры управления идентификаторами;

1.1.3. Правила и процедуры управления средствами аутентификации (аутентификационной информацией);

1.1.4. Правила и процедуры защиты обратной связи при вводе аутентификационной информации;

1.1.5. Правила и процедуры идентификации и аутентификации внешних пользователей;

1.1.6. Правила и процедуры идентификации и аутентификации пользователей, не являющихся работниками Ассоциации.

2. Правила и процедуры идентификации и аутентификации пользователей, являющихся работниками Ассоциации

2.1. Идентификация и аутентификация пользователей, являющихся работниками Ассоциации (далее – внутренние пользователи), должна производиться техническими средствами и системами, содержащими службы каталогов (Microsoft Active Directory, OpenLDAP, Samba и др.).

2.2. К внутренним пользователям относятся должностные лица Ассоциации, выполняющие свои должностные обязанности с использованием информации, информационных технологий и информационной системы и технических средств информационной системы в соответствии с должностными инструкциями и которым в информационной системе также присвоены учетные записи.

2.3. Идентификация внутренних пользователей должна осуществляться по уникальным учетным записям, которые однозначно идентифицируют пользователя. Запрещается применять учетные неидентифицируемые учетные записи, например: «user», «пользователь», «administrator» и т.д. без четкого определения принадлежности учетной записи к субъекту доступа.

2.4. В качестве идентификаторов внутренних пользователей должен использоваться логин службы каталогов.

2.5. Допускается использование иных идентификаторов внутренних пользователей, таких как:

2.5.1. Уникальное устройство (eToken, RuToken, и др.);

2.5.2. Электронная подпись;

2.5.3. Совокупность идентификаторов, указанных в пунктах 2.3 – 2.4 настоящего раздела Правил.

2.6. Для каждого идентификатора должна быть определена следующая информация о пользователе: фамилия, имя, отчество пользователя, должность.

2.7. Учет идентификаторов, выданных внутренним пользователям, производится:

2.7.1. Средствами службы каталогов для идентификаторов, указанных в пункте 2.3 настоящего раздела Правил;

2.7.2. В журнале учета для идентификаторов, указанных в подпункте 2.5.1 пункта 2.5 настоящего раздела Правил;

2.7.3. В журнале учета средств криптографической защиты информации удостоверяющего центра для идентификаторов, указанных в подпункте 2.5.2 пункта 2.5 настоящего раздела Правил.

2.8. Типовые формы учета идентификаторов разрабатываются администратором информационной безопасности (далее – Администратор ИБ).

2.9. Для аутентификации внутренних пользователей могут использоваться следующие факторы аутентификации:

2.9.1. Пароль, пин-код;

2.9.2. Уникальное устройство аутентификации: i eToken, RuToken, смарт-карты и др.

2.10. Допускается в качестве усиления процедур аутентификации использовать комбинации факторов аутентификации информационных систем.

3. Правила и процедуры управления идентификаторами

3.1. Администратор ИБ является лицом, ответственным за создание, присвоение и уничтожение идентификаторов пользователей.

3.2. Запрещается повторно использовать идентификатор пользователя в течение не менее одного года.

3.3. Администратор ИБ обязан блокировать или инициировать блокировку идентификаторов пользователей через период времени неиспользования не более 90 дней.

4. Правила и процедуры управления средствами аутентификации (аутентификационной информацией)

4.1. Администратор ИБ является лицом, ответственным за хранение, выдачу, инициализацию, блокирование средств аутентификации.

4.2. На всех средствах вычислительной техники Администратор ИБ должен осуществлять изменение аутентификационной информации (средств аутентификации), заданной их производителями.

4.3. Администратор ИБ устанавливает и регистрирует в техническом паспорте следующие характеристики паролей:

4.3.1. Длина пароля;

4.3.2. Алфавит пароля (при наличии соответствующих механизмов);

4.3.3. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки программно-технического средства или учетной записи пользователя;

4.3.4. Время блокировки программно-технического средства или учетной записи пользователя после превышения количества неуспешных попыток аутентификации (ввода неправильного пароля);

4.3.5. Максимальное время действия пароля;

4.3.6. Минимальное время действия пароля.

4.4. В случае компрометации или подозрения компрометации паролей, пользователь ИС обязан незамедлительно обратиться к Администратору ИБ.

4.5. Администратор ИБ после сообщения о компрометации обязан осуществить незамедлительное блокирование скомпрометированных средств аутентификации. При необходимости, информация о компрометации сообщается главе администрации района или его заместителю.

4.6.Доступ к администрированию технических средств и систем, содержащим службы каталогов, должен быть предоставлен только Администратору ИБ.

5. Правила и процедуры защиты обратной связи при вводе аутентификационной информации

5.1. Администратор ИБ обеспечивает исключение отображения для пользователя ИС действительного значения аутентификационной информации (пароля) путем:

5.1.1. Использования встроенных средств защиты обратной связи (вводимые символы отображаются условными знаками «*», «|»);

5.1.2. Доработки прикладного программного обеспечения с целью установления средства защиты обратной связи (вводимые символы отображаются условными знаками «*», «|»).

5.2. Пользователю ИС запрещается ввод аутентификационной информации в случае, если существует возможность наблюдения за вводом со стороны посетителей или посторонних лиц.

6. Правила и процедуры идентификации и аутентификации внешних пользователей

6.1. При необходимости в ИС может быть предоставлен доступ внешним пользователям.

6.2. Внешним пользователем ИС является лицо, не относящееся к внутренним пользователям.

6.3. Правила и процедуры доступа внешних пользователей идентичны правилам и процедурам доступа пользователей, являющихся работниками администрации района.

6.4. В качестве дополнительных мер идентификации внешних пользователей для каждого идентификатора должно быть добавлено наименование организации субъекта доступа.

7. Порядок внесения изменений

7.1. Внесение изменений в настоящие Правила осуществляется при изменении правил и процедур идентификации и аутентификации субъектов доступа к объектам доступа.

Приложение № 12
к положению об обработке и обеспечению
безопасности персональных данных
в Ассоциации «Строители Омска»

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей в Ассоциации «Строители Омска»

1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей в Ассоциацию «Строители Омска» (далее – Ассоциация) определяют порядок обработки обращений субъектов персональных данных, поступающих в Ассоциаицю.
2. Субъект персональных данных имеет право на получение сведений, указанных в части 7 статьи 14 Федерального закона Российской Федерации "О персональных данных" (далее - Федеральный закон), за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона.
3. Сведения должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
4. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер и дата заключения договора), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, а также в целях ознакомления с обрабатываемыми персональными данными в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.
6. При обращении субъекта персональных данных или его представителя либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных оператор обязан:
- сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо направить письменный ответ в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя;
- в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного Федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его

представителя либо с даты получения запроса субъекта персональных данных или его представителя;

- предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уничтожить такие персональные данные. Уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

- сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

Приложение № 13

к положению об обработке и обеспечению

безопасности персональных данных

в Ассоциации «Строители Омска»

_____

(фамилия, имя, отчество)

_____

(адрес регистрации с почтовым индексом)

_____

(паспортные данные, орган выдавший паспорт)

_____

(СНИЛС)

_____

(мобильный телефон)

СОГЛАСИЕ

на обработку персональных данных СРО

Я, _____

(фамилия, имя, отчество)

в соответствии с требованиями статьи 9 и на основании пункта 1 части 1 статьи 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в целях формирования дел членов саморегулируемой организации в соответствии с Градостроительным кодексом Российской Федерацим, даю свое согласие Ассоциации «Строители Омска», адрес: 644043, Омская область, город Омск, ул. Красный Путь, дом 101, пом. 72П/5 (далее - Ассоциация) на обработку и совершения с ними соответствующих действий, включая сбор, уточнение (обновление, изменение), запись, передачу, следующих категорий персональных данных:

- фамилия, имя и отчество; гражданство; адрес электронной почты; адрес места жительства (регистрации) или иной адрес для направления заявителю корреспонденции; сведения об образовании; сведения о трудовом стаже; сведения о дополнительном профессиональном образовании (повышении квалификации, профессиональной переподготовке); сведения о разрешении на работу на территории Российской Федерации (для иностранных граждан); сведения об отсутствии (наличии) непогашенной или неснятой судимости;
- дата и место рождения, содержащиеся в справке о наличии (отсутствии) судимости;
- сведения из системы персонифицированного учета органа, осуществляющего индивидуальный (персонифицированный) учет в системе обязательного пенсионного страхования;
- _____

(указать иные предоставляемые по собственной воле персональные данные, требования по предоставлению которых не установлены нормативным правовым актом)

Настоящее согласие дано в момент передачи заявления о приеме в члены Ассоциации «Строители Омска» и приложенных документов и действует бессрочно (если иное не указано ниже).

Я оставляю за собой право отозвать данное согласие посредством составления соответствующего письменного документа, который должен быть направлен в адрес Ассоциации заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Ассоциации. В случае поступления от меня письменного заявления об отзыве персональных данных Ассоциация «Национальное объединение строителей» вправе продолжить обработку персональных данных без согласия субъекта персональных данных до отзыва согласия непосредственно у Ассоциации «Национальное объединение строителей», а также при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

«___»_____ 202___ года _____ _____

(подпись) *(расшифровка подписи)*

Приложение № 14

к положению об обработке и обеспечению

безопасности персональных данных

в Ассоциации «Строители Омска»

_____

(фамилия, имя, отчество)

_____

(адрес регистрации с почтовым индексом)

_____

(паспортные данные, орган выдавший паспорт)

СОГЛАСИЕ

на обработку персональных данных Ассоциацией для внесения в НРС

Я,_____

(фамилия, имя, отчество)

в соответствии с требованиями статьи 9 и на основании пункта 1 части 1 статьи 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в целях ведения национального реестра специалистов в области строительства, даю свое согласие Ассоциации «Национальное объединение строителей», находящейся по адресу: 123242, город Москва, улица Малая Грузинская, дом 3 (далее - Ассоциация), на обработку и совершения с ними соответствующих действий, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, уничтожение следующих категорий персональных данных:

- [дата и место рождения, содержащиеся в справке о наличии (отсутствии) судимости];
- [сведения из системы персонифицированного учета органа, осуществляющего индивидуальный (персонифицированный) учет в системе обязательного пенсионного страхования];
- [указать иные предоставляемые по собственной воле персональные данные, требования по предоставлению которых не установлены нормативным правовым актом].

Ассоциация вправе обрабатывать мои персональные данные посредством внесения в электронные базы данных Ассоциации, хранения бумажных носителей моих персональных данных в специально отведенных для этой цели местах, исключающих несанкционированный доступ к моим персональным данным третьих лиц.

Настоящее согласие дано в момент подачи мной заявления о включении моих персональных данных в национальный реестр специалистов в области строительства и действует бессрочно (если иное не указано ниже).

Я оставляю за собой право отозвать данное согласие посредством составления соответствующего письменного документа, который должен быть направлен в адрес Ассоциации заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Ассоциации. В случае поступления от меня письменного заявления об отзыве персональных данных Ассоциация вправе продолжить обработку персональных данных без согласия субъекта персональных данных только при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

«___»_____ 202_ года _____ _____

(подпись) *(расшифровка подписи)*

АССОЦИАЦИЯ СТРОИТЕЛИ
МСКА

644043, г. Омск,
ул. Красный Путь, 101, пом 72П/5
тел. +7(900)672-99-33

ИНН 5503173432 ОГРН 1175543011731
сайт: строителиомска.рфе-mail: stroiteliomska@yandex.ru

ПРИКАЗ № ПФ-3

г. Омск «20» июня 2019 года

«О назначении лица, ответственного
за обеспечение безопасности персональных
данных в информационной системе»

Во исполнение требований Приказа ФСБ РФ от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Обутверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

ПРИКАЗЫВАЮ назначить лицом, ответственным за обеспечение безопасности персональных данных в информационной системе генерального директора Ассоциации «Строители Омска» Козубович Ольгу Борисовну.

Генеральный директор О.Б. Козубович

С Приказом ознакомлен:

_____

АССОЦИАЦИЯ СТРОИТЕЛИ ОМСКА

644043, г. Омск,
ул. Красный Путь, 101, пом 72П/5
тел. +7(900)672-99-33

ИНН 5503173432 ОГРН 1175543011731
сайт: строителиомска.рфе-mail: stroiteliomska@yandex.ru

ПРИКАЗ № 170-4

г. Омск «13» мая 2019 года

«О назначении комиссии по персональным данным
Ассоциации «Строители Омска»

В целях исполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в целях обеспечения безопасности персональных данных при их обработке в Ассоциации «Строители Омска»

ПРИКАЗЫВАЮ:

1. Утвердить состав комиссии по персональным данным Ассоциации "Строители Омска" в составе:

Болдырев Олег Игоревич – начальник отдела строительного контроля, председатель комиссии;

Ляшенко Алена Николаевна – главный специалист отдела экспертного контроля, заместитель председателя комиссии;

Клим Наталья Николаевна – главный бухгалтер, член комиссии;

Попова Виктория Васильевна – начальник отдела экспертного контроля - юрисконсульт, член комиссии.

2. Комиссии, указанной в пункте 1 приказа, в срок до «31» мая 2019 определить уровни защищенности персональных данных при их обработке в информационных системах Ассоциации «Строители Омска» с оформлением акта.

3. При определении уровня защищенности персональных данных руководствоваться требованиями постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор О.Б. Козубович

С приказом ознакомлены:

Ляшенко А.Н. 20.06.2019
Попова В.В. 20.06.2019
Болдырев О.И. 20.06.2019
Клим Н.Н. 20.06.2019