



**ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«PETRO TEST AVTO»**

**СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА
ОРГАН ПО СЕРТИФИКАЦИИ ПРОДУКЦИИ**



УТВЕРЖДАЮ

Директор ООО «PETRO TEST AVTO»

Т.Э. Раджабов

2020 г.

**ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА
ОБЕСПЕЧЕНИЕ
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ**

ДП СМК ОС 02:2020

РАЗРАБОТАНО

**Представитель руководства
по качеству**

Б.Т. Рузматов

« 05 » 02 2020 г.

Все права интеллектуальной собственности принадлежат ООО «PETRO TEST AVTO» и носит конфиденциальный характер. Содержание данного документа не может воспроизводиться целиком или по частям, либо передаваться третьим лицам, не являющимися сотрудниками предприятия, без предварительного согласования с ПРК. Любые изменения вносятся в оригинал и только в контролируемые копии настоящего документа.

Обозначение документа	ДП СМК ОС 02:2020
Наименование документа	Документированная процедура. Обеспечение конфиденциальности информации
Статус	Действует
Номер редакции	Редакция I
Утвержден и введен в действие	05 февраля 2020 г.
Срок действия	05 февраля 2025 г.
Отметка по истечению срока действия, если нет необходимости их переработки (сведения о продлении срока действия)	Срок действия продлен до «___» _____ 20___ г.
Отметка об актуализации	Актуален до 05 февраля 2021 г.
	Актуален до «05» 02. 2022 г.
	Актуален до «05» 02. 2023 г.
	Актуален до «05» 02. 2024 г.
	Актуален до «05» 02. 2025 г.
Дата последнего изменения	
Разработан впервые	Впервые
Разработан взамен	---
Отметка об изъятии из обращения	«Отменен» от «___» _____ 20___ г.

Отметка о рассылке

№ и количество экземпляров	Наименование подразделения/организации/ответственного лица/	Исх. №, дата сопроводительного документа*	Инициалы, фамилия, получившего документ	Отметка о получении
1	Представитель руководства по качеству	---	Б.Т. Рузматов	<input checked="" type="checkbox"/>
2	Руководитель ОС	---	Т.Э. Раджабов	<input checked="" type="checkbox"/>
3	ГУП «Центр по аккредитации»	Исх. _____ от «___» _____ 2020 г.		<input checked="" type="checkbox"/>

* - заполняется в случае рассылки документа СМК с сопроводительными письмами - обращениями

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА			
ОБЕСПЕЧЕНИЕ			
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ			
ДП СМК ОС 02:2020			
ПСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г.	стр. 1 из 15

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящая документированная процедура (далее – процедура) является документом системы менеджмента качества, разработана в развитие подпунктов «Конфиденциальность» РСМК ОС

с учетом требований пунктов 4.5, 5.2.3, 6.1.1.3, 6.1.3 а), 6.2.2.3, 7.12.2, 8.4.2, А.4.2, А.4.3, А.4.4 к O'z DSt ISO/IEC 17065:2015 и устанавливает порядок обеспечения конфиденциальности информации прав собственности заказчиков услуг.

1.2 Требования настоящей документированной процедуры обязательны для применения **органом по сертификации нефтегазовой и химической продукции** (далее по тексту – ОС) при **Обществе с ограниченной ответственностью «PETRO TEST AVTO»** (далее по тексту – Предприятие).

2 ССЫЛКИ

В настоящей документированной процедуре используются ссылки на следующие документы:

O'z DSt ISO 9000:2016 Системы менеджмента качества. Основные положения и словарь.

O'z DSt ISO/IEC 17065:2015 Государственный стандарт. Оценка соответствия. Требования к органам по сертификации продукции, процессов и услуг.

3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящей документированной процедуре применяются следующие термины с соответствующими определениями, соответствующие O'z DSt ISO 9000, включая следующие термины и определения:

3.1 Информация – значимые данные.

3.2 Конфиденциальность информации – это свойство информации быть известной только аутентифицированным законным субъектам системы.

3.3 Доступность информации – это свойство информации быть доступной для аутентифицированных законных субъектов системы.

3.4 Целостность информации – это свойство информации быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий.

3.5 Разглашение конфиденциальности информации – действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо, вопреки трудовому или гражданско-правовому договору.

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА			
ОБЕСПЕЧЕНИЕ			
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ			
ДП СМК ОС 02:2020			
РСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г.	стр. 2 из 15

3.6 Незаконное использование конфиденциальности информации

– возмездная или целенаправленная передача конфиденциальности информации другим лицам без согласия Предприятия, либо принятие различных решений и осуществление действий на основе конфиденциальной информации в интересах Сотрудника или не соответствующих принципам деловой этики, принятой Предприятием.

4 ОБОЗНАЧЕНИЯ, СОКРАЩЕНИЯ И АББРЕВИАТУРЫ

В настоящей документированной процедуре применяются следующие обозначения, сокращения и аббревиатуры:

- БН** – бумажный носитель;
- ГУП** – Государственное унитарное предприятие;
- ООО** – Общество с ограниченной ответственностью;
- ОС** – орган по сертификации;
- IDT** – идентичный стандарт;
- ЭН** – электронный носитель.

5 ОТВЕТСТВЕННОСТЬ И ПОЛНОМОЧИЯ

5.1 Руководитель ОС несет ответственность, за:

- осуществление контроля над доступом посторонних лиц к бумажным и электронным носителям.

- соблюдение сотрудниками ОС, а также привлекаемыми специалистами, профессиональной тайны в отношении конфиденциальной информации, которую они получают в результате взаимоотношений с Заявителями, предоставившими материалы на сертификацию продукции по подтверждению соответствия в области деятельности ОС, представленной в приложении к свидетельству об аккредитации.

5.2 Менеджер по качеству несет ответственность, за:

- инструктирование о запрете разглашения соответствующей информации и об ответственности за ее разглашения.

5.3 Стороны (Заявитель и ОС) несут ответственность за:

- обеспечение сохранности конфиденциальной информации и нести ответственность за незаконное собирание, разглашение и/или использование конфиденциальной информации в соответствии с законом РУз.

5.4 Сотрудники ОС несут ответственность за:

- за незаконное получение, разглашение и/или использование информации, составляющих коммерческую тайну. Сотрудники несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с действующим законодательством РУз;

- сотрудники, которые в связи с исполнением трудовых обязанностей получили доступ к информации, составляющей коммерческую тайну, обладателями, которой является Предприятие и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА			
ОБЕСПЕЧЕНИЕ			
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ			
ДП СМК ОС 02:2020			
РСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г.	стр. 3 из 15

отсутствии в действиях такого работника состава преступления несут дисциплинарную ответственность в соответствии законодательством РУз;

- сотрудники не несут ответственность, если разглашение коммерческой тайны Предприятия произошло не по их вине.

6 ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

6.1 Общие положения

Политика и цели по отношению обеспечения конфиденциальности информации

Цели защиты конфиденциальности информации:

- соблюдение конфиденциальности информации ограниченного доступа;

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к такой информации, а также иных неправомерных действий в отношении такой информации;

- реализация конституционного права граждан на доступ к информации;

- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование.

Политика по отношению обеспечения конфиденциальности информации

При получении доступа к информации, необходимой для проведения эффективных мероприятий по оценке соответствия, наш ОС гарантирует, что конфиденциальность ее будет сохранена. Это осуществляется подписанием соглашения о конфиденциальности или включением требований о соблюдении конфиденциальности в основной договор на оказание услуг по подтверждению соответствия.

Все организации и лица имеют право на защиту любой коммерческой информации, обозначенной ее собственником как «Конфиденциальная», которую они предоставляют нашей ОС для проведения работ по оценке соответствия.

Наш ОС добровольно принимает договорные обязательства по соблюдению конфиденциальности и отвечает за управление всей информацией обозначенной ее собственником как «Конфиденциальная», полученной или созданной во время мероприятий по оценке соответствия.

Мы, обязуемся заранее сообщать заявителю об информации, которую мы используем, какую часть этой информации мы намереваемся сделать достоянием гласности, за исключением той информации, которую сам заявитель сделал общественным достоянием или которая согласована договорными обязательствами между заявителем и нашим ОС.

В случае, когда ОС требуется в соответствии с законодательством или в соответствии с полномочиями, полученными согласно договорным обязательствам, раскрыть конфиденциальную информацию, заявитель или заинтересованное лицо будут в обязательном порядке уведомлены о

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА			
ОБЕСПЕЧЕНИЕ			
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ			
ДП СМК ОС 02:2020			
РСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г.	стр. 4 из 15

предоставлении информации, если это не запрещено законодательствами РУз.

Информация о заявителе, полученная как из других источников, так и от самого заявителя, в нашей ОС считается конфиденциальной по умолчанию и разглашению не подлежит.

Весь персонал ОС сохраняет конфиденциальность всей информации, полученной или созданной в ходе выполнения работ по подтверждению соответствия, кроме случаев, предусмотренных законодательством РУз. Соблюдение персоналом конфиденциальности обеспечивается подписанием с каждым сотрудником, участвующим в оценке соответствия, Соглашения о конфиденциальности.

ОС располагает и использует средства для обеспечения безопасности при работе с конфиденциальной информацией и объектами оценки соответствия. Для этого в компании существует ответственный работник контролирующей работу сотрудников с конфиденциальной информацией.

Ответственность за соблюдение конфиденциальности лежит на высшем руководстве Предприятия, а также персонально на каждом из сотрудников. В случае неправомерных действий по использованию конфиденциальной информации ОС и сотрудники несут ответственность в соответствии с законами РУз.

Доведение Политики до сведения персонала ОС, осуществляется:

- путем ознакомления персонала, в т.ч. и привлекаемых, с Политикой на общих собраниях;
- при приеме на работу новых сотрудников;
- методом наглядной агитации.

Доведение Политики до Заявителей услуг ОС, Заявителей, посетителей осуществляется путем публикации соответствующей информации на стендах, плакатах, размещение Политики на сайте Предприятия и другими способами.

Политика вывешена на стенде в помещении ОС и доступна в любое время для изучения всем сотрудникам.

ОС разрабатывает и реализует меры по предотвращению и разрешению возникающих конфликтов интересов.

Соглашение о конфиденциальности информации оформляется на каждого сотрудника ОС. Повторное ознакомление проводится не реже 1 раза в год, о чём, делается запись в документе.

Форма Соглашения о конфиденциальности информации приведена в приложение А.

6.2 Процедура защиты электронного хранения и передачи результатов

Проблема обеспечения безопасности имеет три аспекта: конфиденциальность, целостность и доступность.

6.2.1 Конфиденциальность

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА		
ОБЕСПЕЧЕНИЕ		
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ		
ДП СМК ОС 02:2020		
РСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г. стр. 5 из 15

ОС обеспечивает конфиденциальность информации, путем открывания доступа к информации, только аутентифицированным пользователям. ОС ограждает электронные документы, хранящиеся в системе (компьютере) от атак доступа. ОС учитывает различные способы представления информации – в виде распечаток, файлов или пакетов, передающихся по сетям.

Существуют различные способы обеспечения конфиденциальности документов в зависимости от их вида.

Бумажные документы защищаются физически, т.е. хранятся в отдельном месте, доступ к которому контролируется менеджером по качеству и/или руководителем ОС.

Примечание:л

Не следует забывать о таких вещах, как запирающие шкафы, ящики столов, ограничение доступа в кабинеты внутри ОС или в саму ОС.

В работе с электронными документами соблюдаются следующее:

- допускается хранение файлов одновременно в нескольких местах: на внешних запоминающих устройствах большой емкости (жестких дисках или магнитных лентах), на гибких дисках, zip-дисках или компакт-дисках.

- физический доступ к месту хранения файлов не обязателен.

Сохранение конфиденциальности магнитных лент и дисков аналогично защите бумажных документов и связано с ограничением физического доступа.

Примеры механизмов обеспечения конфиденциальности файлов и требования, которые к ним предъявляются, указаны в таблице 1.

Таблица 1 – Механизмы обеспечения конфиденциальности файлов и требования к ним

Механизмы обеспечения конфиденциальности	Контроль физической безопасности
	Контроль доступа к файлам на компьютере
	Шифрование файлов
Требования к конфиденциальности файлов	Идентификация
	Правильная настройка компьютерной системы
	Правильное управление ключами при использовании шифрования

6.2.2 Доступность

ОС компьютерные системы поддерживает в готовности к работе, позволяет обращаться к компьютерным системам, хранящимся в этих системах данным и приложениям.

ОС обеспечивает передачу информации между компьютерными системами, где хранятся информация, в электронной форме.

Для сохранения важной информации самым простым способом является создание ее резервных копий и размещение их в безопасном месте. Для этой цели копии важных документов хранятся как на бумажном носителе, так и на электронных носителях (например, на флеш картах). Резервные копии предотвращают полную потерю информации при случайном или преднамеренном уничтожении файлов.

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА		
ОБЕСПЕЧЕНИЕ		
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ		
ДП СМК ОС 02:2020		
РСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г. стр. 6 из 15

В наличие резервных копий для безопасности они хранятся в сейфах или изолированных помещениях, в которые ограничен физический доступ лиц.

Право доступа к документам ОС и компьютерной базе данных имеют:

- те специалисты ОС, работа которых требует знания этой информации;

- лица, проводящие государственный контроль или аудит.

Копирование документов по подтверждению соответствия продукции производится с разрешения руководителя ОС с предупреждением директора Предприятия.

Правом беспрепятственного получения любой информации обладает директор предприятия.

Выдача документов для проверяющих органов осуществляется только с разрешения директора.

6.2.3 Целостность

Руководитель ОС и ее сотрудники для обеспечения целостности следят за правильностью информации.

Информация может быть представлена в виде бумажных распечаток или в виде файлов.

В целях защиты бумажных документов от подделки, ставиться подпись на каждой странице (в случаях, когда это предусмотрено процедурой) и/или сшиваются документы в папки.

Основным способом защиты целостности документов в электронных носителях контроль над доступом к файлам на компьютере. С помощью механизма управления доступом установлено для файла разрешение «только для чтения» и запрещена запись изменений. Для этого случая пользователя, который хочет внести изменения - правильно идентифицирован.

6.3 Соблюдения конфиденциальности при сотрудничестве ОС с Заявителями

ОС при сотрудничестве с Заявителями в вопросах разъяснения запроса Заявителя обязуется обеспечить конфиденциальность по отношению к другим Заявителям.

В целях вышеуказанного в ОС разработана Политика соблюдения конфиденциальности, где отражены необходимые обязательства.

Сотрудники соблюдают принципами деловой этики, в целях чего подписывают соглашение по этическим нормам.

Соглашение по этическим нормам оформляется на каждого сотрудника ОС. Повторное ознакомление проводится не реже 1 раза в год, о чём, делается запись в документе.

Форма соглашения по этическим нормам приведена в приложение В.

6.4 Порядок обеспечения конфиденциальности информации и защиты прав собственности заявителей

6.4.1 Обеспечение конфиденциальности информации

ОС обеспечивает конфиденциальность информации, полученной в ходе проведения сертификационных работ, в том числе от третьих лиц, на

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА		
ОБЕСПЕЧЕНИЕ		
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ		
ДП СМК ОС 02:2020		
РСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г. стр. 7 из 15

всех уровнях ее деятельности, включая свои подразделения и сотрудников, как штатных и работающих по совместительству, так и от работающих по трудовому договору (соглашению о сотрудничестве) с ОС, в соответствии с действующим законодательством РУз.

В ОС принимаются меры, исключающие утечку информации, составляющей коммерческую тайну, получаемой от изготовителей и организаций в ходе деятельности ОС, которая может нанести материальный и моральный ущерб заявителю, снизить конкурентоспособность изделия, за исключением конечных результатов, а также вопросов, касающихся требований безопасности, путем выполнения следующих процедур:

- хранят в сейфе, шкафу или в рабочем столе: журналы регистрационные, пакет документов по сертификации продукции, письма, договора, комплекты материалов аккредитации, носители электронной информации, содержащие секретные сведения;

- соблюдают метод входа по паролю в компьютер, хранящий информацию о результатах сертификационных работ, тем самым защищая конфиденциальность информации, содержащейся на электронных носителях;

- не разглашают результаты сертификационных работ третьим лицам (кроме последнего абзаца данного пункта);

- не проводят сертификационные работы в присутствии посторонних лиц, за исключением внутренних аудиторов, назначенных приказом директора предприятия;

- не передают информацию по сертифицируемым объектам и результатам испытаний третьим лицам, не имеющим соответствующих полномочий по доступу к информации;

- сохраняют в течение установленного срока конфиденциальность информации и прав собственности её заказчиков;

- все материалы и документы, полученные от Заявителя, хранятся в Архиве в специально отведенных папках;

- дело (папка) каждого заказчика, содержащее полученные от него документы, результаты сертификационных работ хранятся в Архиве;

- соблюдают другие меры по сохранению конфиденциальности и защите прав собственности заказчиков;

- несут административную ответственность за нарушение пунктов вышеуказанных процедур.

Только информация, полученная в процессе сертификационных работ, негативно влияющая на здоровье и безопасность людей, их имущество или окружающую среду, а также другая информация, раскрытие которой предусмотрено законом или стандартом доводится до третьей стороны, о чем сообщается заявителю.

6.4.2 Объектом конфиденциальности в работе ОС является следующая информация заявителей:

- сведения о технологии и организации производства, «ноу-хау», сведения о перспективных разработках продукции, коммерческие данные

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА			
ОБЕСПЕЧЕНИЕ			
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ			
ДП СМК ОС 02:2020			
ПСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г.	стр. 8 из 15

и любые другие, которые могут представить интерес для конкурентов Заявителя;

- сведения о недостатках, несоответствиях, материальных трудностях и любые другие, которые могли бы повредить престижу Заявителя, принести ему моральный и материальный ущерб;

- объем производимой продукции, ее стоимость, поставщик, место хранения;

- технологические инструкции и регламенты, применяемые оборудования;

- сведения об учредителях и собственниках;

- прочая информация, особо оговоренная Заявителем.

Специальные требования к составу конфиденциальной информации (при их наличии со стороны Заявителя) оформляются при заключении договора на оказание услуг ОС.

6.4.3 Перечень документов, являющихся конфиденциальными:

- учредительные и финансово-экономические документы;

- регистрационные и рабочие журналы (записи);

- документы по подтверждению соответствия продукции.

6.4.4 Система обеспечения конфиденциальности информации включает в себя следующее:

- до каждого из сотрудников ОС, участвующего в процессе сертификационных работ, менеджером по качеству доводятся сведения о соблюдении конфиденциальности информации, полученной при осуществлении своей деятельности;

- исключение доступа посторонних лиц к технической документации;

- ограничение информации о сертификационных работах, допуском к ней только лиц, непосредственно проводящих данную работу, и лиц, занимающихся оформлением документов по сертификации. Разрешение на допуск к указанным материалам других сотрудников может быть дано только руководителем ОС с предупреждением директора Предприятия;

- разглашение сотрудниками ОС конфиденциальной информации, полученной в процессе сертификационных работ, рассматривается как грубое нарушение трудового договора (или заключенного с сотрудниками ОС гражданско-правового договора) и невыполнение им должностных обязанностей, что влечет за собой дисциплинарные взыскания вплоть до расторжения трудового договора (или заключенного с сотрудниками ОС гражданско-правового договора).

Информация об отдельной продукции Заявителя, не должна раскрываться третьему лицу без письменного разрешения Заявителя. Если закон требует предоставления информации третьему лицу, Заявитель информируется о передаче такой информации, как это предусмотрено законодательством РУз.

Без разрешения заявителя ОС в рекламе своей деятельности не указывает, что он проводит (проводил) какие-либо работы для него.

После проведения сертификационных работ комплект документации остается в ОС и становится его собственностью. При этом ОС принимает

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА			
ОБЕСПЕЧЕНИЕ			
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ			
ДП СМК ОС 02:2020			
РСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г.	стр. 9 из 15

на себя обязательства не передавать документацию другим организациям и хранить ее так, чтобы был исключен доступ посторонних лиц. Документы по результатам сертификационных работ, оформленные ОС, передаются Заявителю, и является его собственностью.

В случаях, когда руководителям и специалистам ОС при осуществлении деятельности становится известной информация о персональных данных, необходимо руководствоваться законодательством РУз, регулирующим отношения, связанные с защитой, обработкой, организацией хранения, комплектования, учета и использования персональных данных.

7 ДОКУМЕНТИРОВАНИЕ

Перечень документов приведенных в данной процедуре указаны в Таблице 2.

Таблица 2

№ п/п	Наименование документа	вид* документа
1	2	3
01	Политика и цели о соблюдения конфиденциальности	(ЭН/БН)
02	Соглашение о конфиденциальности	(ЭН/БН)
03	Соглашение по этическим нормам	
<p><i>*ЭН – документ хранится на электронном носителе;</i> <i>БН - документ хранится на бумажном носителе</i></p>		

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА			
ОБЕСПЕЧЕНИЕ			
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ			
ДП СМК ОС 02:2020			
РСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г.	стр. 10 из 15

**Приложение А
(обязательное)**

ДП СМК ОС 02-А

СОГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ

В период работы нижеподписавшегося сотрудника в аккредитованном органе по сертификации продукции (далее по тексту – ОС) при Обществе с ограниченной ответственностью «PETRO TEST AVTO», данный сотрудник будет/был ознакомлен, и/или владел конфиденциальной информацией, включая, но не ограничиваясь конфиденциальной технологией, усовершенствованиями, списками Заявителей, прейскурантом цен, методами работы, знанием и данными, относящимися к процессам, услугам ОС.

Характер работы достаточно конкурентный, и раскрытие любой конфиденциальной информации приведёт серьёзным проблемам для ОС, которые будет трудно соизмерить.

В период работы и после ухода из ОС при ООО «PETRO TEST AVTO», нижеподписавшийся сотрудник:

- будет хранить конфиденциальность и не раскроет никакую информацию конфиденциального характера;

- не будет никогда, прямо или косвенно, использовать какую-либо конфиденциальную информацию для любой цели, выходящей за пределы работы такого сотрудника в ОС;

- не раскрывать любую конфиденциальную информацию физическому или юридическому лицу без предварительного письменного разрешения руководства ООО «PETRO TEST AVTO».

Более того, но без ограничения, такой сотрудник никогда не будет копировать, передавать, публиковать или проводить какое-либо коммерческое или другое использование любой конфиденциальной информации без предварительного письменного согласия руководства ООО «PETRO TEST AVTO».

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА			
ОБЕСПЕЧЕНИЕ			
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ			
ДП СМК ОС 02:2020			
РСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г.	стр. 11 из 15

Ознакомлен и согласен

_____	_____	_____
инициалы, фамилия	подпись	дата

Повторное ознакомление:

_____	_____	_____
инициалы, фамилия	подпись	дата

_____	_____	_____
инициалы, фамилия	подпись	дата

Приложение В (обязательное)

ДП СМК ОС 02-В

СОГЛАШЕНИЕ по ЭТИЧЕСКИМ НОРМАМ

Я, согласен(а) при выполнении моих обязанностей в аккредитованном органе по сертификации продукции (далее по тексту – ОС) при Обществе с ограниченной ответственностью «PETRO TEST AVTO» строить своё поведение и работу на принципах честности и соблюдения **этических** норм, полностью соответствующих **этической** политике ОС.

ИСКЛЮЧАТЬ СЛУЧАИ:

- 1) Преднамеренного утаивания любых происшествий, несчастных случаев или примеров неэтичной работы, противоречащих этической политике.
- 2) Использования служебного положения в целях оказания давления на подчинённых для осуществления любых действий, противоречащих этическим нормам, а также этической политике ОС.
- 3) Разглашения конфиденциальной информации, полученной в процессе сертификационных работ.
- 4) Выдача любой организации или клиентам данных сертификационных работ или наблюдений, не являющихся прямым результатом выполнения стандартной процедуры, а также любых намёков о том, что ОС может предоставлять такие услуги.
- 5) Преднамеренной фальсификации любых данных, отчётов или положений относящихся к любой деятельности ОС, области деятельности или результатам сертификационных работ.
- 6) Преднамеренной записи и выдачи руководству данных, не являющихся результатом выполнения стандартной процедуры и сертификационных работ.
- 7) Преднамеренного сокрытия известных деталей любого инцидента, деловой практики или несчастных случаев, или невыполнения работы согласно стандартной деловой практике.
- 8) Использования неутверждённой или сокращённой процедуры, которые могут исказить точность/качество выдаваемых результатов сертификационных работ.

НЕСУ ОТВЕТСТВЕННОСТЬ

За соблюдение законодательство, выполнять свои должностные или служебные обязанности беспристрастно, объективно, добросовестно, с соблюдением правил этического поведения и воздерживаться от совершения каких-либо коррупционных правонарушений или любых других действий, создающих условия для совершения таких правонарушений.

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА		
ОБЕСПЕЧЕНИЕ		
КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ		
ДП СМК ОС 02:2020		
РСМК ОС 01:2020 п. 6.5	Редакция I	Дата введения: 05.02.2020 г. стр. 12 из 15

В ЦЕЛЯХ РАСКРЫТИЯ И УРЕГУЛИРОВАНИЯ КОНФЛИКТА ИНТЕРЕСОВ Я ОБЯЗАН:

- соблюдать требования, указанные в ПКИ СМК 01:2020 «Положение о конфликте интересов»;
- при принятии решений по деловым вопросам и выполнении своих трудовых обязанностей руководствоваться интересами ОС;
- без учета своих личных интересов, интересов своих родственников и друзей;
- избегать (по возможности) ситуаций и обстоятельств, которые могут привести к конфликту интересов;
- раскрывать возникший (реальный) или потенциальный конфликт интересов;
- содействовать урегулированию возникшего конфликта интересов.

СОГЛАСЕН:

1) Немедленно информировать моего непосредственного руководителя о любых попытках работы, противоречащих этической политике ОС.

2) Сообщать моему непосредственному руководителю или аудитору о выдаче любых данных, которые не являются результатом выполнения стандартных процедур или сертификационных работ, в зависимости от того, производилась ли их выдача преднамеренно или непреднамеренно, мной или другим сотрудником ОС.

Ознакомившись с настоящим этическим соглашением, сознаю, что несоблюдение описанных выше условий повлечёт за собой дисциплинарное взыскание вплоть до увольнения из ОС.

Ознакомлен и согласен

инициалы, фамилия	подпись	дата
-------------------	---------	------

Повторное ознакомление:

инициалы, фамилия	подпись	дата
-------------------	---------	------

инициалы, фамилия	подпись	дата
-------------------	---------	------

