Утверждаю
Генеральный директор
ОАО «РСП ТПК КГРЭС»
_____ М.В. Езжев
«__1__»_____ 2013 г

ИНСТРУКЦИЯ
о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

1. Общие положения

1.1. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее – Инструкция), является обязательной для всех структурных подразделений ОАО «РСП ТПК КГРЭС».
1.2. Под персональными данными понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в т. ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, доходы и др.
1.3. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных, а также в отношении общедоступных персональных данных.
В общедоступные источники персональных данных (в т. ч. справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, сведения о профессии, абонентский номер
1.4. Конфиденциальность персональных данных предусматривает обязательное получение согласия субъекта персональных данных (наличие иного законного основания) на их обработку.
Согласие не требуется на обработку данных:

- необходимых для доставки почтовых отправлений организациями почтовой связи;
- включающих в себя только фамилию, имя и отчество субъекта;
- данных, работа с которыми проводится в целях исполнения обращения (запроса) субъекта персональных данных, трудового или иного договора с ним, однократного пропуска в здание или в иных аналогичных целях;
- обработка которых осуществляется без средств автоматизации.

1.5. Порядок ведения перечней персональных данных в структурных подразделениях ОАО «РСП ТПК КГРЭС» утверждается локальным актом.
Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.
1.6. Все работники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны иметь допуск (разрешение) к работе с соответствующими видами персональных данных.
1.7. Работникам, осуществляющим обработку персональных данных, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью, а также оставлять материальные носители с персональными данными без присмотра в незапертом помещении. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа должны переноситься подготовившим их работником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

1.8. Передача персональных данных допускается только в случаях, установленных Федеральными законами от 27.07.2006 № 152-ФЗ "О персональных данных" и от 02.05.2006 № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации", действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.
1.9. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством РФ и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.
1.10. Ответственность за защиту обрабатываемых персональных данных возлагается на работников подразделений ОАО «РСП ТПК КГРЭС», осуществляющих такую обработку по договору с оператором, а также на иные лица, осуществляющие обработку или хранение конфиденциальных данных в ОАО «РСП ТПК КГРЭС». Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную и уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами.

2. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых без использования средств автоматизации

2.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна быть организована таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения материальных носителей персональных данных и установить перечень лиц, осуществляющих обработку.
2.2. При хранении материальных носителей необходимо соблюдать условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах выполнения такой обработки.
2.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается на одном материальном носителе размещать персональные данные, цели обработки которых заведомо не совместимы. Для обработки персональных данных каждой категории должен использоваться отдельный материальный носитель.
2.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, и невозможности обработки одних персональных данных отдельно от других, зафиксированных на том же носителе, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.
2.5. Уничтожение или обезличивание всех или части персональных данных (если это допускается материальным носителем) производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых с использованием средств автоматизации

3.1. Безопасность персональных данных при их обработке в информационных системах, хранении и пересылке обеспечивается с помощью системы защиты персональных данных, включающей специальные средства защиты информации, а также используемые в информационной системе информационные технологии.

3.2. Допуск лиц к обработке персональных данных в информационных системах осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

3.3. Работа с информационными системами должна быть организована таким образом, чтобы обеспечить сохранность носителей персональных данных и средств защиты информации, а также исключить возможность неконтролируемого пребывания в помещениях, где они находятся, посторонних лиц.

3.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из шести и более символов.

3.5. Работа на компьютерах с персональными данными без паролей доступа или под чужими или общими (одинаковыми) паролями, а также пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в т. ч. сети Интернет, запрещается.

3.6. При обработке персональных данных в информационных системах пользователями должно быть обеспечено:

-использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

-недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

-постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

-недопущение несанкционированного выноса из помещений, установки и подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.7. При обработке персональных данных в информационных системах разработчики и администраторы систем должны обеспечивать:

-обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

-учет лиц, допущенных к работе с персональными данными в информационных системах, прав и паролей доступа;

-учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

-контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

описание системы защиты персональных данных.

3.8. Специфические требования к защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

3.9. Работники подразделений ОАО «РСП ТПК КГРЭС» и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку.

Приложение №1

Сведения об обработке персональных данных работников ОАО «РСП ТПК КГРЭС», осуществляемой **без использования средств автоматизации** в

_____

(наименование структурного подразделения)

Перечень обрабатываемых персональных данных (указать наименование типовой формы или вида документов – картотека, журнал, книга. реестр и т.д.)	Цель обработки персональных данных	ФИО и должность лиц, ответственных за обработку и хранение персональных данных	Место хранения (корпус, кабинет, сейф, специально оборудованный шкаф и др.)	ФИО и должность лиц, имеющих доступ к просмотру персональных данных

«___»_____20____ г. _____/_____

(Подпись) (Ф.И.О. руководителя подразделения)

Приложение №2

Сведения об обработке персональных данных работников ОАО «РСП ТПК КГРЭС», осуществляемой **с использованием средств автоматизации** в

_____

(наименование структурного подразделения)

Перечень обрабатываемых персональных данных (указать наименование типовой формы или вида документов – картотека, журнал, книга. реестр и т.д.)	Цель обработки персональных данных	ФИО и должность лиц, ответственных за обработку и хранение персональных данных	Наименование информационной системы с указанием используемых программных средств. Место установки (корпус, кабинет)	Исходные данные классификации информ. системы				ФИО администратора информационной системы	ФИО и должность лиц, имеющих доступ к просмотру персональных данных
				Структура инф.системы (распределенная, автономная, локальная)	Наличие подключений к сетям общего пользования (да, нет)	Режим обработки персонал. Данных (многопользовательский, однопользовательский)	Разграничение доступа пользователей (да, нет)		

«___»_____20____ г. _____/_____

(Подпись) (Ф.И.О. руководителя подразделения

Приложение №3

ЖУРНАЛ

учета съемных носителей персональных данных

_____

(наименование структурного подразделения)

Начат «__» _____ 20___ г.

Окончен «__» _____ 20___ г.

_____

Должность и ФИО ответственного за хранение

_____

Должность и ФИО администратора

№ п/п	Наименование и номер съемного носителя	Фамилия исполнителя	Действие (Получил, вернул, проверил)	Дата и время действия	Подпись исполнителя	Подпись ответственного за хранение
1						
2						
3						
4						
5						

«УТВЕРЖДАЮ»
Генеральный директор
ОАО «РСП ТПК КГРЭС»
_____М.В. Езжев
«___»_____ 20__г.

АКТ
уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом генерального директора №___ от __ _____ 20__ в составе:
1. _____
2. _____
3. _____

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

№ п/п	Дата	Учетный номер съемного носителя	Пояснения

Всего съемных носителей_____
(цифрами и прописью)
На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации _____ (механического уничтожения, сжигания и т.п.).
Перечисленные съемные носители уничтожены путем_____ (разрезания, демонтажа и т.п.), измельчены и сданы для уничтожения предприятию по утилизации вторичного сырья .

_____ _____
(наименование предприятия) (Дата)

Председатель комиссии Подпись Дата
Члены комиссии
(ФИО) Подпись Дата