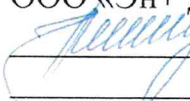


Стандарт предприятия

О защите конфиденциальной информации

Введен впервые

УТВЕРЖДАЮ
Генеральный директор
ООО «Эн+ Диджитал»
 А. А. Герасименко
10.10.2018
(дата)

Введен в действие приказом ООО «Эн+
Диджитал»
от 08.10.18г. № 23

ООО «Эн+ Диджитал»

Содержание

Содержание	2
Введение	3
1. Область применения	3
2. Нормативные ссылки	3
3. Сокращения и определения	3
4. Общие положения	5
5. Права обладателя конфиденциальной информации	6
6. Обеспечение режима конфиденциальности информации	7
7. Определение перечня сведений, относящихся к КИ, в том числе коммерческой тайне.	8
8. Ограничение доступа к конфиденциальной информации. Средства и методы	9
9. Организация технической защиты информации	11
10. Обязанности руководителей, подразделений и работников по выполнению требований защиты конфиденциальной информации	11
11. Порядок обращения с конфиденциальными документами и носителями информации	12
12. Ответственность за нарушение режима конфиденциальности (коммерческой тайны)	17
Приложение 1	19
Приложение 2	21
Приложение 3	24
Приложение 4	25
Приложение 5	26
Приложение 6	27
Приложение 7	28
Приложение 8	29
Приложение 9	31
Приложение 10	32
Лист регистрации изменений	33

Введение

Настоящий стандарт предприятия разработан в соответствии с действующими законодательством РФ и нормативными документами ООО «Эн+ Диджитал» (далее Компания).

1. Область применения

1.1. Настоящий стандарт распространяется на информацию конфиденциального характера (составляющую коммерческую тайну), независимо от вида носителя, на котором она зафиксирована.

1.2. Настоящий стандарт предприятия входит в состав нормативных документов системы управления Компании.

2. Нормативные ссылки

2.1. В настоящем стандарте использованы ссылки на следующие документы:

- Указ Президента от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- Федеральный закон РФ от 29.09.2004 № 98-ФЗ «О коммерческой тайне».
- СТП 011.473.128-2010 «Политика в области информационной безопасности».
- СТР-К 2002г Специальные требования и рекомендации по технической защите конфиденциальной информации.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

3. Сокращения и определения

3.1. В настоящем стандарте используются следующие сокращения:

КИ - Конфиденциальная информация;
КТ - Коммерческая тайна;
КЗ – Контролируемая зона;
ДЗР – Дирекция по защите ресурсов;
ЗП – защищаемые помещения.

3.2. В настоящем стандарте используются следующие определения:

Безопасность информации – состояние защищенности информации, характеризующееся способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от юридических и физических лиц, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Обладатель конфиденциальной информации – юридическое или физическое лицо, которое владеет конфиденциальной информацией на законном основании, ограничило доступ к этой информации и установило в отношении неё режим конфиденциальности (коммерческой тайны).

Владелец КИ (КТ) – должностное лицо (руководитель структурного подразделения), наделенное обладателем КИ правами владения, пользования и ответственностью в отношении КИ в полном или ограниченном объеме.

Режим конфиденциальности, коммерческой тайны – правовые, организационные, технические и иные меры, принимаемые обладателем конфиденциальной информации, в т.ч. составляющей коммерческую тайну, по охране ее конфиденциальности.

Доступ к конфиденциальной информации – ознакомление персонала Компании и других лиц с конфиденциальной информацией, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации от несанкционированного доступа – деятельность по предотвращению получения защищаемой информации юридическими и физическими лицами с нарушением нормативных актов или правил доступа к защищаемой информации, утвержденных в Обществе.

Информация – сведения о предметах, объектах, явлениях, процессах (независимо от формы их представления).

Информация, составляющая коммерческую тайну – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим конфиденциальности (коммерческой тайны).

Контрагент – сторона гражданско-правового договора.

Конфиденциальная информация (в т.ч. составляющая коммерческую тайну) – не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам и содержащиеся в перечне сведений конфиденциального характера, доступ к которым ограничивается в соответствии с законодательством РФ.

Коммерческая тайна (КТ) – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Контролируемая зона (КЗ) – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Мероприятие по защите информации – совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

Обязательство о неразглашении конфиденциальной информации (коммерческой тайны) – письменное обязательство работника Компании о неразглашении конфиденциальной информации, составляющей коммерческую тайну, которое подписывается при оформлении на работу.

Компания – ООО «Эн+ Диджитал», а также партнеры, являющиеся пользователями или администраторами информационных систем ООО «Эн+ Диджитал», подписавшие соответствующие соглашения.

Подразделения ИБ – подразделение (работник), ответственное за контроль обеспечения ИБ Общества, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.

Система защиты информации от несанкционированного доступа к информации – комплекс организационных мер и программно-технических (при необходимости криптографических) средств защиты от несанкционированных действий с конфиденциальной информацией.

Техническая защита конфиденциальной информации – защита информации не криптографическими методами, направленными на предотвращение утечки защищаемой

информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования.

Предоставление (передача) Конфиденциальной информации – передача КИ, зафиксированной на материальном носителе ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления, контрагентам в целях выполнения их функций или договорных обязательств в объеме и на условиях, которые предусмотрены договором, включая условие о принятии установленных мер по охране ее конфиденциальности.

Разглашение конфиденциальной информации – действие или бездействие, в результате которых КИ, 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.

Структурные подразделения – филиалы, дирекции, управления, отделы, службы, а также другие подразделения Компании.

4. Общие положения

4.1. Целью соблюдения правил обращения с конфиденциальной информацией является предотвращение утечки конфиденциальной информации, обеспечение ограниченного доступа к носителям этой информации, создание условий сохранности и защиты от несанкционированного доступа.

4.2. Настоящий стандарт регулирует отношения, связанные с отнесением информации к конфиденциальной информации, передачей такой информации, охраной ее конфиденциальности в целях выполнения Федеральных Законов, обеспечения интересов Компании и предупреждения недобросовестной конкуренции, а также неоправданных финансово-экономических затрат, расходов.

4.3. Перечень сведений конфиденциального характера утвержден указом Президента от 13 июля 2015 г. № 357:

4.3.1. сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные).

4.3.2. сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом.

4.3.3. служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна –ДСП, для служебного пользования).

4.3.4. сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

4.3.5. сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

4.3.6. сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

4.3.7. сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом

от 2 октября 2007 г. N 229-ФЗ «Об исполнительном производстве».

4.4. Информация, которая не может составлять коммерческую тайну Компании в соответствии с законодательством Российской Федерации на основании Федерального закона РФ от 29.09.2004г. № 98ФЗ «О коммерческой тайне»:

4.4.1. содержащаяся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

4.4.2. содержащаяся в документах, дающих право на осуществление предпринимательской деятельности;

4.4.3. о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4.4.4. о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

4.4.5. о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

4.4.6. о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

4.4.7. о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

4.4.8. об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

4.4.9. о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

4.4.10. о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

4.4.11. обязательность раскрытия, которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

4.4.12. общедоступная информация (включая положения, правила, инструкции, цены и тарифы), доведение которой до партнеров и контрагентов обязательно для Компании в соответствии с действующим законодательством Российской Федерации или нормативными документами Компании.

5. Права обладателя конфиденциальной информации

5.1. Обладатель КИ, имеет право:

5.1.1. устанавливать, изменять и отменять в письменной форме режим конфиденциальности (коммерческой тайны) в соответствии с настоящим стандартом;

5.1.2. использовать КИ для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

5.1.3. разрешать или запрещать доступ к КИ, определять порядок и условия доступа к этой информации;

5.1.4. требовать от юридических и физических лиц, получивших доступ к КИ,

органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена КИ, соблюдения обязанностей по охране ее конфиденциальности;

5.1.5. требовать от лиц, получивших доступ к КИ, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации;

5.1.6. защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами КИ, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

5.2. Права обладателя КИ, возникают с момента установления им в отношении такой информации режима конфиденциальности (коммерческой тайны).

5.3. Право на отнесение информации к КИ и на определение перечня и состава такой информации принадлежит обладателю информации с учетом настоящего стандарта.

5.4. Обладателем КИ в рамках настоящего стандарта является Компания.

6. Обеспечение режима конфиденциальности информации

6.1. Меры по защите конфиденциальной информации, в том числе коммерческой тайны, принимаемые в Обществе:

6.1.1. определение перечня сведений, составляющих КИ, в том числе коммерческую тайну;

6.1.2. определение информационных ресурсов, содержащих конфиденциальную информацию, а также мест обращения, хранения носителей этой информации;

6.1.3. ограничение доступа к конфиденциальной информации, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

6.1.4. учет лиц, получивших доступ к конфиденциальной информации;

6.1.5. регулирование отношений по использованию конфиденциальной информации, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

6.1.6. регистрация носителей (документы, магнитные, оптические, электронные носители и т.п.), содержащих конфиденциальную информацию или отнесенную к КИ с указанием полного наименования обладателя этой информации – Компании или его контрагента

6.2. Порядок регистрации, обращения и хранения носителей конфиденциальной информации, охватывается правилами обращения с конфиденциальной информацией.

6.3. Владелец КИ вправе применять по согласованию с Подразделением ИБ средства и методы технической защиты этой информации и другие, не противоречащие законодательству Российской Федерации, меры по ее защите.

6.4. Меры защиты и обеспечения информационной безопасности должны отвечать следующим требованиям:

6.4.1. непрерывность защиты, с целью использования наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывного контроля ее состояния, выявления узких и слабых мест и противоправных действий;

6.4.2. плановость защиты, путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели Компании;

6.4.3. целенаправленность защиты, для защиты информации в рамках конкретной цели, утрата которой может причинить Компании ущерб;

6.4.4. надежность защиты по перекрытию возможных путей неправомерного

доступа и использования информации, подлежащей защите, независимо от формы ее представления и вида физического носителя;

6.4.5. универсальность защиты, с целью защиты информации независимо от вида канала утечки или способа несанкционированного доступа;

6.4.6. для защиты должны применяться комплексные меры, включающие все доступные виды и формы защиты в полном объеме.

6.5. При выработке мер защиты должны учитываться требования к:

6.5.1. управлению физической защитой и контролю доступа;

6.5.2. управлению техническими средствами;

6.5.3. управлению вычислительными системами и сетями;

6.5.4. управлению персоналом;

6.5.5. управлению непрерывностью бизнеса;

6.5.6. управлению инцидентами информационной безопасности;

6.5.7. аудиту информационной безопасности.

7. Определение перечня сведений, относящихся к КИ, в том числе коммерческой тайне.

7.1. Отнесение сведений к КИ, в том числе коммерческой тайне, выполняется на основе предложений от структурных подразделений Компании. Перечень сведений, относящихся к КИ, утверждается руководителем Компании.

7.2. Присвоение документу грифов «Конфиденциально», «Коммерческая тайна» осуществляется его исполнителем при согласовании с непосредственным руководителем, подписывающим или утверждающим этот документ в соответствии с Перечнем сведений, содержащих КИ Компании. Если сведения, содержащиеся в документе, не относятся к конфиденциальной информации, а характер и важность проблемы, проявление интереса со стороны конкурентов к нему и другие факторы вызывают необходимость закрытия содержащейся в нем информации, исполнитель вправе присвоить данному документу гриф «Коммерческая тайна» и через руководителя соответствующего подразделения обратиться в подразделение, ответственное за конфиденциальный документооборот, с предложением об отнесении данного документа к категории КТ.

7.3. При отнесении информации к КИ, в том числе коммерческой тайне, должны выделяться следующие основные признаки:

7.3.1. сведения не являются общеизвестными;

7.3.2. к ним не относится информация, представляющая чисто научный интерес (идеи, не дающие прибыль);

7.3.3. является активным ресурсом, сравнимым с энергоресурсами, материальными запасами;

7.3.4. используется для производства товаров, услуг;

7.3.5. имеет стоимость, может продаваться, теряет стоимость во времени, не будучи реализованной;

7.3.6. из всей собственности Компании, в том числе и имущественной, может быть наиболее ценной;

7.3.7. может быть получена без всяких затрат или с малыми усилиями;

7.3.8. реально или потенциально создает преимущества Компании в конкурентной борьбе;

7.3.9. в отношении которой владельцем такой информации введен режим

конфиденциальности (коммерческой тайны).

8. Ограничение доступа к конфиденциальной информации. Средства и методы

8.1. Доступ к конфиденциальной информации, должен быть ограничен как на физическом (доступ в помещения, где циркулирует, обрабатывается или хранится информация) так и на логическом уровне (к базам данных, автоматизированным системам).

8.2. Руководители структурных подразделений на основе перечня Сведений конфиденциального характера и перечня КИ Компании проводят инвентаризацию информационных ресурсов на наличие в них конфиденциальной информации, формируют реестр и письменно представляют его в Подразделение ИБ. Одновременно определяются места обработки и хранения (в т.ч. техническими средствами) конфиденциальной информации.

8.3. Средства и методы защиты формируются и устанавливаются с учётом СТР-К 2002г. и других нормативных документов специалистами Подразделения ИБ на основе реестра, представленного от структурных подразделений Компании.

8.4. Защищаемые помещения, где циркулирует, обрабатывается и хранится конфиденциальная информация, должны размещаться в пределах контролируемой территории предприятия. При этом, рекомендуется размещать их на максимальном удалении от границ контролируемой территории. Ограждающие конструкции (стены, полы, потолки) не должны являться смежными с помещениями других учреждений (предприятий).

8.5. Границей КЗ могут являться:

8.5.1. периметр охраняемой территории учреждения (предприятия);

8.5.2. ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

8.6. В отдельных случаях на период обработки техническими средствами конфиденциальной информации КЗ временно может устанавливаться большей, чем охраняемая территория предприятия. При этом должны приниматься организационно-режимные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

8.7. Не рекомендуется располагать защищаемые помещения на первых этажах зданий.

8.8. Для исключения просмотра текстовой и графической конфиденциальной информации через окна помещения рекомендуется оборудовать их шторами (жалюзи).

8.9. Во время проведения совещаний, в помещениях, где циркулирует информация конфиденциального характера, запрещается использование средств радиосвязи (радиотелефонов, оконечных устройств сотовой, WiFi, транкинговой связи), переносных магнитофонов и других средств аудио и видеозаписи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком или спикерфоном, а также аппаратов с автоматическим определителем номера, следует отключать их из сети на время проведения этих мероприятий.

8.10. Отправление конфиденциальных документов и ведение конфиденциальных переговоров разрешается только по защищенным от несанкционированного доступа каналам связи (включая ведомственные АТС, корпоративные информационные системы и т.п.).

8.11. По решению руководителя Компании (генерального директора, директора, директора филиала) и согласованию с Подразделением ИБ специальная проверка ЗП и

установленного в нем оборудования может проводиться сторонними организациями, имеющими соответствующие лицензии ФСБ.

8.12. Контроль эффективности защиты информации в защищаемых помещениях и каналах связи возлагается на Подразделение ИБ.

8.13. Защищаемые помещения оборудуются средствами охранно-пожарной сигнализации и сдаются на пульт охраны, неконтролируемое пребывание посторонних лиц в них запрещается.

8.14. Доступ работников Компании и контрагентов к КИ.

8.15. К материалам и документам, содержащим конфиденциальную информацию, допускаются: руководящий состав Компании и работники Компании только в случае производственной необходимости и подписавшие обязательство о неразглашении таковой. (Образец Обязательства - Приложение 1.)

8.16. Составление списка должностных лиц, которым необходим допуск к документам и информационным массивам, содержащим конфиденциальную информацию, возлагается на руководителей структурных подразделений Компании.

8.17. Допуск сотрудников Компании к конфиденциальной информации (в т.ч. КТ) согласовывается с Подразделением ИБ и обязательно отражается в трудовом договоре и в должностной инструкции. Руководители структурных подразделений подготавливают и передают взятые обязательства о неразглашении конфиденциальной информации для хранения в личном деле работника.

8.18. Отдел по управлению персоналом (кадровые подразделения филиалов) извещают подразделение, ответственное за конфиденциальный документооборот, об увольнении работников, обращающихся с конфиденциальной информацией, до издания приказа об увольнении.

8.19. Допуск работников других юридических лиц к документам и информационным массивам, составляющим КИ.

8.20. Допуск работников государственных органов, юридических лиц к документам и информационным массивам Компании, составляющим КИ, осуществляется в следующем порядке:

8.20.1. для органов государственной власти - на основании законодательства и нормативных актов РФ по мотивированному запросу, направленному на имя генерального директора Компании.

8.20.2. для контрагентов – с обязательным заключением договора о неразглашении конфиденциальной информации, утвержденного генеральным директором Компании, или по его решению.

8.21. Отношения между обладателем КИ, и его контрагентом в части, касающейся охраны конфиденциальности информации, регулируются договором.

8.22. В договоре должны быть определены условия охраны конфиденциальности информации, в том числе в случае реорганизации или ликвидации одной из сторон договора в соответствии с гражданским законодательством, а также обязанность контрагента по возмещению убытков при разглашении им этой информации вопреки договору.

8.23. В случае, если иное не установлено договором между обладателем КИ и контрагентом, контрагент в соответствии с законодательством Российской Федерации самостоятельно определяет способы защиты КИ, переданной ему по договору.

8.24. Контрагент обязан незамедлительно сообщить обладателю КИ, о допущенном им либо ставшем ему известном факте разглашения или угрозы разглашения, незаконном

получении или незаконном использовании такой информации третьими лицами.

8.25. Контрагент до окончания срока действия договора не может разглашать КИ, а также в одностороннем порядке прекращать охрану ее конфиденциальности, если иное не установлено договором.

8.26. Контрагент по окончании срока действия договора обязан прекратить обработку (любое действие с информацией или бездействие по обеспечению её конфиденциальности включая хранение, извлечение, использование, передачу, ознакомление) КИ и уничтожить её в срок не превышающий тридцати дней с даты окончания срока договора, если иное не предусмотрено договором.

8.27. Конфиденциальная информация, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

8.28. Конфиденциальная информация считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации мер по охране конфиденциальности этой информации. При этом получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация относится к конфиденциальной информации или составляет коммерческую тайну, и что осуществляющее передачу этой информации лицо не имеет законного основания на передачу этой информации.

9. Организация технической защиты информации

9.1. Мероприятия по защите информации техническими средствами осуществляется специалистами по информационной безопасности Подразделения ИБ после документального определения перечня защищаемых помещений, определения ответственных лиц за их эксплуатацию и обязательного специального обследования ЗП. Специальные обследования помещения предусматривают выявление технических каналов утечки информации с учётом объективных и субъективных факторов в соответствии с ГОСТ Р 51275-2006 и Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К 2002 г.).

9.2. По результатам обследования подготавливается акт с указанием выявленных и возможных каналов утечки информации. Требования, указанные в акте обследования, если не оговорено специально, являются обязательными на всех стадиях проектирования, строительства, оснащения, эксплуатации ЗП.

10. Обязанности руководителей, подразделений и работников по выполнению требований защиты конфиденциальной информации

10.1. Трудовые обязанности руководителей и подразделений по организации в структурных подразделениях режима конфиденциальности информации (коммерческой тайны):

10.1.1. подача предложения об отнесении информации к КИ Компании;

10.1.2. организация постоянного контроля за информационными ресурсами, содержащими конфиденциальную информацию;

10.1.3. определение должностных лиц подразделения, которым необходим доступ к КИ и согласование его с Подразделением ИБ;

10.1.4. назначение ответственного работника за конфиденциальное делопроизводство на вверенном направлении деятельности и организация регистрации и хранения носителей информации;

10.1.5. организация доступа к КИ работникам Компании и сторонним организациям

в объёме, необходимом им для выполнения своих обязанностей или работ по договору;

10.1.6. организация выполнения мероприятий по технической защите КИ.

10.2. Общие обязанности работников Компании по выполнению установленного режима конфиденциальности информации (коммерческой тайны) указаны в соглашении между работником и Компанией о неразглашении конфиденциальной информации:

10.2.1. не разглашать конфиденциальную информацию (коммерческую тайну), и без согласия руководства Компании не использовать эту информацию в личных целях;

10.2.2. не разглашать конфиденциальную информацию и коммерческую тайну, обладателями которой являются Компания и его контрагенты, после прекращения трудового договора в течение срока, предусмотренного соглашением между работником и Компанией;

10.2.3. возместить причиненный Компании ущерб, в случае вины в разглашении информации, составляющей коммерческую тайну, ставшей ему известной в связи с исполнением им трудовых обязанностей;

10.2.4. передать Компании при прекращении или расторжении трудового договора, имеющиеся в пользовании материальные носители информации, содержащие конфиденциальную информацию;

10.2.5. немедленно сообщать своему непосредственному руководителю об утрате, порче, недостатке или несанкционированном доступе ненадлежащих лиц к сведениям, имеющих конфиденциальный характер;

10.2.6. после окончания рабочего времени убирать документы, относящиеся к конфиденциальной информации в закрытое от доступа посторонним лицам место (запираемый на замок сейф, металлический ящик, шкаф);

10.2.7. сообщать в ДЗР о любых нарушениях режима конфиденциальности (коммерческой тайны).

11. Порядок обращения с конфиденциальными документами и носителями информации

11.1. Конфиденциальный документооборот является неотъемлемой частью требований по защите КИ.

11.2. Ведение конфиденциального документооборота ведётся ответственными за конфиденциальное делопроизводство, назначенными приказом руководителя Компании/филиала, отдельно от обычного документооборота. Допускается ведение в электронном виде реестра приема/передачи документов с указанием регистрационных номеров, но без указания содержания документов.

11.3. Ответственные за конфиденциальный документооборот несут персональную ответственность за сохранность и учёт КИ.

11.4. Регистрации подлежит вся поступившая на предприятие корреспонденция или полученная работниками от сторонних организаций информация с пометкой ограничения доступа (К, КТ, ДСП...). Корреспонденция принимается и вскрывается ответственным за конфиденциальный документооборот. Корреспонденция, поступившая на имя руководителя предприятия с пометкой «Лично», регистрируется в журнале учёта пакетов и передается руководителю без вскрытия пакета/конверта под роспись. После вскрытия конверта руководитель предприятия принимает решение о регистрации документа и необходимости передачи документа на исполнение.

11.5. При приеме конвертов (пакетов) с конфиденциальной информацией, проверяется правильность доставки корреспонденции по адресу, целостность упаковки, оттисков печатей и наличие указанных в документах приложений, а также соответствие

номеров полученных документов указанным на конвертах.

11.6. Приём, передача носителей с КИ осуществляется под роспись в журналах учета входящих, исходящих документов или учёта носителей КИ. Допускается, при необходимости, передача КИ по реестру или акту приема-передачи КИ.

11.7. Хранение КИ в электронном виде осуществляется с применением средств криптографической защиты, с использованием средств разграничения доступа или на отчуждаемом носителе информации. Допускается, как исключение, хранение КИ на ПК в заархивированном с паролем файле. Пароль к архиву должен соответствовать требованиям стандарта «Управление паролями». Запрещается хранить КИ в электронном виде без применения средств защиты.

11.8. В случае утраты носителей, разглашении КИ, об инциденте немедленно ставится в известность Подразделение ИБ. Руководителем Компании назначается служебное расследование, которое проводит представитель Подразделения ИБ с обязательным привлечением работника подразделения по управлению персоналом. В регистрационных журналах учёта КИ ставится соответствующая отметка. В случае, если был утрачен единственный экземпляр документа, принимаются меры для его восстановления.

11.9. Учёт журналов

11.9.1. Журнал «Учёт журналов» (приложение №3) заполняется ответственным за конфиденциальный документооборот.

11.9.2. В журнале «Учёт журналов» ведется учет всех журналов, их передача, подготовка на архивное хранение и уничтожение.

11.10. Учёт носителей конфиденциальной информации

11.10.1. При взятии носителей на учёт ответственный за конфиденциальный документооборот заполняет графы 1-4 журнала «Учёт носителей конфиденциальной информации» (Приложение №4). После взятия на учет носитель передается исполнителю с заполнением граф 6, 7 журнала.

11.10.2. В графе 3 журнала «Учёт носителей конфиденциальной информации» проставляются типы носителей, на которые перенесена информация (жесткие диски, flash-диски, магнитные, оптические носители и др.), и их учётные номера.

11.10.3. В формах учёта носителей не должны производиться подчистки и исправления с применением корректирующей жидкости. Ошибочная запись зачеркивается одной чертой. Вносимые изменения заверяются подписью ответственного за конфиденциальный документооборот с проставлением даты.

11.11. Разработка конфиденциального документа.

11.11.1. Разработка проекта конфиденциального документа осуществляется исполнителем в соответствии с общими требованиями к документированию управленческой деятельности и организации работы с документами, установленными стандартами Компании, лицом, имеющим соответствующий допуск.

11.11.2. Документы, разрабатываемые исполнителем на ПК, формируются, хранятся, группируются в папки и защищаются с использованием средств защиты.

11.11.3. Основанием для разработки конфиденциального документа может являться указание (письменное, устное), резолюция.

11.11.4. После разработки проект документа и все его незарегистрированные копии уничтожаются исполнителем.

11.12. Учёт изданных конфиденциальных документов.

11.12.1. Подлинный документ и его копии учитываются в журнале «Учёт

подготовленных и изданных конфиденциальных документов» (приложение №5).

11.12.2. При приёме документа от исполнителя ответственный за конфиденциальный документооборот:

- проверяет правильность оформления документа;
- присваивает учетный номер документу;
- заполняет графы 1-8 журнала «Учёт подготовленных и изданных конфиденциальных документов»;
- если документ отправляется, заполняются графы 9, 10;
- передает документ исполнителю под подпись в графе 11 журнала «Учёт подготовленных и изданных конфиденциальных документов».
- в верхнем правом углу документа проставляет – гриф конфиденциальности, штамп КТ (вх, исх, рег) уч. № с указанием номера.

11.13. Отправление изданных конфиденциальных документов.

11.13.1. При отправлении конфиденциальных документов нарочным ответственный за конфиденциальный документооборот оформляет реестр на отправляемую корреспонденцию (Приложение №9) и передает его вместе с отправляемыми документами исполнителю. Получение документов подтверждается адресатом отметкой в реестре (дата, подпись, ФИО и должность получившего). Реестр сдается исполнителем ответственному за конфиденциальный документооборот, о чем делается отметка в журнале «Учёт подготовленных и изданных конфиденциальных документов».

11.13.2. Почтовая отправка конфиденциальных документов осуществляется через Первый отдел исполнительной дирекции (в филиалах – через спецчасти по ГО-ЧС и мобилизационной работе). Допускается отправка почтовой или курьерской службой, с которой заключен договор, предусматривающий соблюдение условий конфиденциальности. Передача конфиденциальных документов для отправки производится в законвертованном виде. Конверты должны быть светонепроницаемые. Отправка нескольких документов, направляемых одному адресату, осуществляется в одном пакете.

11.13.3. На пакете проставляются следующие реквизиты:

- гриф конфиденциальности (в правом верхнем углу);
- ниже грифа (при необходимости) отметка «Лично»;
- адрес и наименование предприятия-получателя;
- при наличии отметки «Лично» - должность, инициалы, фамилия адресата;
- под адресатом – учетные номера документов, вложенных в пакет; при наличии сопроводительного письма – только номер письма; при отправлении нескольких экземпляров – напротив учетных номеров проставляются номера экземпляров;
- адрес и наименование предприятия-отправителя
- при необходимости в центре верхнего поля – «Срочно»

11.13.4. При помещении документов в подготовленные пакеты проверяется соответствие данных на документах и пакетах.

11.13.5. При отправлении конфиденциальных документов почтовой или курьерской службой исполнитель получает в подразделении документационного обеспечения управления копию квитанции об отправке и передает ответственному за конфиденциальный документооборот.

11.13.6. Об отправленных документах производятся отметки в графах соответствующих учетных форм:

- в журнале «Учёт подготовленных и изданных конфиденциальных документов» графы 9,10;
- в журнале «Учет поступивших конфиденциальных документов» (приложение №6) в графе 12 (пересылка).

11.14. Учёт поступивших конфиденциальных документов.

11.14.1. Поступившие пакеты конфиденциальных документов передаются ответственному за конфиденциальный документооборот.

11.14.2. При вскрытии пакетов проверяется:

- соответствие на пакете и документах отправителя и адресата;
- гриф конфиденциальности;
- номера документов и экземпляров;
- наличие листов в документах, наличие и количество листов приложений.

11.14.3. При несоответствии на пакете и документе или на документе и приложениях учетных номеров, недостатке или излишке листов и экземпляров составляется акт в 2-х экземплярах. Второй экземпляр вместе с лицевой стороной пакета направляется отправителю, сообщается руководителю. Ошибочно присланные документы, лишние листы и экземпляры вместе с актом направляются с сопроводительным листом в новом пакете отправителю. Об этом делается отметка в графе 12 журнала «Учёт поступивших конфиденциальных документов» с указанием количества листов, номера экземпляров и причина, номер и дата сопроводительного письма.

11.14.4. После вскрытия пакета ответственный за конфиденциальный документооборот:

- присваивает документам очередные порядковые номера по журналу «Учёт поступивших конфиденциальных документов» и проставляет их в графе 1;
- в графе 4 проставляет номер, присвоенный документу на предприятии, издавшем документ;
- для документов без сопроводительного письма: в графе 6 – количество листов документа, в графе 7 – прочерк; для документов с сопроводительным письмом: в графе 6 – количество листов сопроводительного письма, в графе 7 – количество листов приложений (если все приложения имеют гриф – проставляется общее количество листов приложений, если часть не имеет грифа – количество листов проставляется через знак «+» к листам конфиденциальных приложений с аббревиатурой н/к (не конфиденциальных)). Для нескольких экземпляров проставляется количество в графе 5.
- проставляет в правом углу нижнего поля отметку о получении на самом документе (учётный номер, присвоенный документу, гриф конфиденциальности, дата поступления). Например:

Уч. № 48КТ
19.05.2017

на всех приложениях (на первом листе) в правом углу делает отметку «КТ уч. №», присвоенному при регистрации.

11.14.5. При возвращении ранее отправленных документов, зарегистрированных по любому виду учёта, ответственный за конфиденциальный документооборот в соответствующих формах учета (в графе 13 журнала «Учёт изданных конфиденциальных документов», при необходимости, в графе 6 журнала «Учёт носителей конфиденциальной информации») делает запись «Экз. № _____ возвращен, п/ж № _____ за _____».

11.14.6. Документ, возвращенный с сопроводительным письмом, регистрируется за очередным номером в журнале «Учёт поступивших конфиденциальных документов».

11.14.7. После регистрации ответственный за конфиденциальный документооборот предварительно рассматривает документы и передает их руководству для рассмотрения и оформления резолюции/выдачи поручений в соответствии с установленными стандартами Компании под подпись в журнале «Учёт поступивших конфиденциальных документов».

11.14.8. Документы, предназначенные только для ознакомления, не выдаются исполнителю, ознакомление с документом производится у ответственного за конфиденциальный документооборот, с отметкой в «Листе ознакомления» (приложение №7).

11.14.9. Передача конфиденциальных документов от руководства в структурные подразделения, между структурными подразделениями или между работниками в ходе исполнения производится только с фиксацией передачи в журнале «Учёт поступивших конфиденциальных документов» или в карточке-заместителе конфиденциального документа (приложение № 8).

11.15. Хранение и работа с конфиденциальными документами.

11.15.1. Работающий с конфиденциальными документами в течение дня работник при выходе из кабинета убирает документы в сейф (запирающийся металлический шкаф). При выходе из кабинета всех работников дверь закрывается на ключ.

11.15.2. Исполненные документы находятся на хранении в структурном подразделении или, по решению руководителя, передаются ответственному за конфиденциальный документооборот.

11.15.3. При увольнении исполнитель передает через ответственного за конфиденциальный документооборот все находящиеся у него конфиденциальные документы другому работнику, который определяется руководителем подразделения, либо сдает их в подразделение конфиденциального делопроизводства.

11.15.4. Выдача исполненных документов, находящихся на хранении у ответственного за конфиденциальный документооборот, для ознакомления производится по письменному запросу с заведением карточки-заместителя.

11.16. Копировально-множительные работы.

11.16.1. Размножение конфиденциальных документов должно производиться только при действительной служебной необходимости в их дополнительных экземплярах, подтвержденной документально (письмо, служебная записка и т.д.).

11.16.2. При изготовлении копии конфиденциального документа на первом листе над реквизитом «Гриф ограничения доступа» проставляется слово КОПИЯ, либо в нижней части листа проставляется штамп КОПИЯ ВЕРНА с подписью ответственного за конфиденциальный документооборот.

11.16.3. При изготовлении копии конфиденциального документа ей присваивается отдельный учетный номер – очередной порядковый номер по журналу «Учет подготовленных и изданных конфиденциальных документов».

11.17. Подготовка конфиденциальных документов для уничтожения.

11.17.1. Для подготовки к выделению документов к уничтожению создается экспертная комиссия, которая должна состоять из ответственного за конфиденциальный документооборот, работника службы безопасности и работников подразделений, где ведется обработка конфиденциальных документов.

11.17.2. После утверждения описи документов постоянного и временного срока хранения составляется акт (приложение №10) о выделении документов за соответствующий период к уничтожению. В акт включаются отобранные экспертной комиссией для уничтожения документы. Гриф конфиденциальности акта должен соответствовать совокупной степени конфиденциальности сведений, содержащихся в документах. Акт с грифом регистрируется в журнале учёта подготовленных и изданных конфиденциальных документов.

11.17.3. Каждый документ и учётный журнал вносятся в акт отдельной позицией и должны соответствовать данным о них, зафиксированным в протоколе экспертной комиссии и учётных формах.

11.17.4. Листы документов и учётные карточки просчитываются, сложенные документы разворачиваются. Соответствие данных заверяется в акте подписями проверяющих.

11.17.5. Уничтожение документов и учётных журналов должно производиться путём сжигания или с помощью shreddera. При уничтожении документов вне территории предприятия доставка их к месту уничтожения производится на служебном транспорте, и принимаются меры, исключающие доступ к документам посторонних лиц.

11.17.6. После уничтожения производится отметка об уничтожении документов и учётных журналов.

11.17.7. Составление акта о выделении к уничтожению документов, учётных журналов и проставлении в учётных формах отметок об их уничтожении осуществляются ответственным за конфиденциальный документооборот. В проверке правильности включения в акт документов, учётных журналов и в их физическом уничтожении, кроме этого работника должны участвовать члены экспертной комиссии.

11.18. Проверка наличия конфиденциальных документов и носителей.

11.18.1. Целью проверок наличия конфиденциальных документов является обеспечение контроля за сохранностью документов и выявление неучтенных по каким-либо причинам конфиденциальных документов, установление этих причин и взятие таких документов на учет путем установления соответствия фактического наличия документов учетным данным на них, выявление отсутствующих документов и принятия мер по их розыску.

11.18.2. Для обеспечения контроля проводятся следующие виды проверок:

- проверки правильности проставления регистрационных данных носителей, документов и учётных журналов;
- проверки правильности проставления отметок о движении носителей, документов;
- проверки фактического наличия всех носителей и изданных и поступивших документов;
- нерегламентированные проверки фактического наличия документов, которые проводятся по мере возникновения необходимости в них: при смене руководителя и сотрудников подразделения конфиденциального делопроизводства, их временном отсутствии (болезнь, командировка, отпуск), временном отсутствии исполнителей, нарушении оттисков печатей на хранилищах документов, ликвидации предприятия.

12. Ответственность за нарушение режима конфиденциальности (коммерческой тайны)

12.1. В случае нарушения установленного режима конфиденциальности (коммерческой тайны) или разглашения сведений, составляющих коммерческую тайну, работник Компании может быть привлечен к дисциплинарной, гражданско-правовой, административной, уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

12.2. Работники Компании несут ответственность:

12.2.1. за использование информации, составляющую КИ, в том числе коммерческую тайну в публикациях, открытых документах, выступлениях, переписке, рекламных материалах и информационных сообщениях;

12.2.2. за передачу документов, содержащих КИ в любом виде, посторонним лицам, если это не связано с производственной необходимостью и не санкционировано руководителем подразделения;

12.2.3. за передачу КИ, по незащищенным каналам связи, ведение переговоров в непригодных помещениях;

12.2.4. за разглашение сведений о перечне находящихся у них носителей информации, составляющей КИ, системе их защиты и месте хранения;

12.2.5. за вынос любых носители информации, составляющей КИ из здания Компании без письменного разрешения руководителя структурного подразделения.

12.2.6. за изготовление несанкционированных копий (распечатку, запись на диктофон, сканирование, фотографирование и т.д.) с материальных носителей (документов), относящихся к КИ.

Обязательство о неразглашении конфиденциальной информации (коммерческой тайны) «Компании»

Я (Ф.И.О.) _____

как (должность, подразделение) _____

уведомлён и осознаю, что получил доступ к информационным ресурсам, собственником которых является ООО «Эн+ Диджитал», в дальнейшем «Компания».

Я подтверждаю, что вся деловая информация, и, прежде всего, отнесённая руководством Компании к служебной и конфиденциальной информации, представляют собой особо ценный капитал Компании, а защита его является неотъемлемой частью кредитно-финансовой, коммерческой деятельности.

На основании изложенных убеждений, обязуюсь:

1. В период работы в Обществе ни прямо, ни косвенно не разглашать сведения, составляющие конфиденциальную информацию или коммерческую тайну Компании, которые мне будут доверены или станут известны при исполнении служебных обязанностей, за исключением, когда передача третьим лицам, опубликование или другое разглашение сведений, может осуществляться с разрешения, данного мне руководством Компании в установленном порядке.

2. Использовать прямо или косвенно информацию, содержащую конфиденциальную информацию или служебную информацию не иначе, чем в интересах выполнения своих служебных обязанностей по заданию или в целях и интересах Компании.

3. Строго соблюдать требования по защите конфиденциальной информации, сосредоточенной на бумажных и электронных носителях, в каналах связи, при работе в информационной сети Компании и сети Интернет.

Я предупрежден, что при использовании корпоративных технических средств радиопроводной связи и информационных технологий мои действия могут быть подконтрольны *Дирекции по защите ресурсов* в части обеспечения безопасности Компании, предотвращения утечки конфиденциальной информации, а также целевого использования информационных ресурсов/систем и предоставляемых услуг связи ООО «Эн+ Диджитал».

4. Осуществлять деловые связи с отечественными и зарубежными партнерами строго в объеме делегированных мне полномочий.

5. В случае попытки посторонних лиц получить от меня сведения конфиденциального характера, немедленно сообщить об этом руководству Компании.

6. В период работы в Обществе не работать и не участвовать без предварительного согласия руководства в деятельности сторонних организаций, учреждений и предприятий, конкурирующих с Компанией и (или) являющихся контрагентами Компании.

Я подтверждаю, что не имею перед каким-либо лицом или организацией обязательств, которые входят в противоречие с положениями настоящего документа, или которые ограничивают мою деятельность в интересах Компании.

Мне известно, что в случае нарушения мною установленного в соответствии с настоящим обязательством и *Перечнем сведений, составляющих коммерческую тайну*, режима защиты этой информации в ООО «Эн+ Диджитал», я возмещаю причиненный моими действиями ущерб в порядке, предусмотренном действующим законодательством РФ, а также теряю доверие и право лояльного отношения к себе руководства Компании, что может быть основанием для принятия решения о расторжении со мной Трудового договора (контракта) или привлечения к ответственности в соответствии с законодательством РФ.

Со Стандартами предприятия по обеспечению защиты конфиденциальной информации и перечнем сведений составляющих конфиденциальную информацию и коммерческую тайну Компании ознакомлен_(а).

_____ 20__ г.

_____/подпись/

Администрация Компании подтверждает, что данные Вами обязательства не ограничивают Ваших прав на интеллектуальную собственность.

Об окончании срока действия обязательства администрация ООО «Эн+ Диджитал» уведомит Вас заблаговременно в письменной форме.

Личную подпись _____ подтверждаю.

(ФИО взявшего на себя обязательство)

Начальник отдела (службы), филиала

ООО «Эн+ Диджитал»

/ _____ /

“ ____ ” _____ 20__ г.

Образец Договора со сторонними организациями

Конфиденциально

Экз. № _____

ДОГОВОР**о неразглашении конфиденциальной информации**

г. Иркутск

«___» _____ 20__ г.

ООО «Эн+ Диджитал», именуемое в дальнейшем Передающая сторона, в лице генерального директора _____, действующего на основании Устава, с одной стороны, и _____, именуемое в дальнейшем Получающая сторона, в лице _____, должность, Ф.И.О. _____, действующего на основании (Устава, доверенности и т.д.), с другой стороны, в дальнейшем именуемые Стороны, заключили настоящий договор, в дальнейшем именуемый "Договор", о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1. Передающая сторона передает Получающей стороне документы, содержащие конфиденциальную информацию, необходимую для исполнения Получающей стороной своих обязательств по договору от «___» _____ 20__ г. № _____ для ООО «Эн+ Диджитал», а Получающая сторона обязуется обеспечить конфиденциальность этой информации в соответствии с условиями настоящего Договора.

2. ОБЯЗАННОСТИ СТОРОН

2.1. Передающая сторона передает документы, содержащие запрашиваемую информацию, по запросу Получающей стороны. При этом на документах, передаваемых в рамках настоящего Договора и содержащих конфиденциальную информацию, в правом верхнем углу проставляется гриф "конфиденциально" или "коммерческая тайна".

2.2. Получающая сторона обязуется направлять запрос с перечнем документов и сведений, составляющих конфиденциальную информацию, с указанием номера и даты подписания Договора на выполнение работ для ООО «Эн+ Диджитал», цель использования запрашиваемых документов или сведений (далее по тексту договора Запрос) и список лиц которые будут допущены к полученным документам (сведениям). Запрос направляется в адрес Дирекции по безопасности и режиму Передающей стороны.

2.3. Получающая сторона обязуется не разглашать конфиденциальную информацию, полученную ею от Передающей стороны, какому-либо третьему лицу, и использовать эту информацию исключительно для достижения цели, указанной в Запросе.

2.3. Получающая сторона обязуется соблюдать в отношении полученной ею от Передающей стороны конфиденциальной информации во избежание ее разглашения или использования такую степень секретности, какую Получающая сторона соблюдала бы в разумной степени в отношении своей собственной конфиденциальной информации такой же степени важности. Получающая сторона обязуется обеспечить режим коммерческой тайны в работе с переданными документами и выделить для их получения и работы с ними сотрудников, взявших на себя обязательства по сохранности переданной информации. Перечень указанных сотрудников оформляется в виде Приложения № 1 к настоящему Договору, являющегося неотъемлемой его частью.

2.4. Информация не считается конфиденциальной и Получающая сторона не несёт никаких обязательств перед Передающей стороной в отношении данной информации, если она удовлетворяет одному из следующих условий:

1) до момента передачи документов, содержащих запрошенную информацию, эта информация получена Получающей стороной от третьей стороны без нарушения действующего законодательства Российской Федерации и настоящего Договора;

2) информация на момент ее передачи является публично известной в результате неправильного, небрежного или намеренного действия Передающей стороны, или становится таковой после ее передачи;

3) представлена третьей стороне Передающей стороной без аналогичного ограничения на права третьей стороны;

4) независимо разработана Получающей стороной, при условии, что лицо или лица, работавшие ее, не имели доступа к конфиденциальной информации;

5) разрешена к выпуску письменным разрешением Передающей стороны.

2.5. Получающая сторона обязана письменно сообщить об обстоятельствах, указанных в подпунктах 1-5 пункта 2.4 настоящего Договора, в противном случае она лишается права ссылаться на данные обстоятельства в случае привлечения её к ответственности за разглашение конфиденциальной информации.

2.6. Вся информация, передаваемая Передающей стороной Получающей Стороне в письменной форме согласно настоящему Договору, является исключительной собственностью Передающей стороны. Переданные документы и любые их копии должны быть возвращены Передающей стороне в течение 10 дней со дня достижения цели, указанной в запросе, оформленной по настоящему Договору, если иное не будет предусмотрено соглашением сторон.

2.7. Стороны обязуются не разглашать факт существования и условия настоящего Договора без предварительного письменного согласия другой стороны.

2.8. Если третья сторона предпримет в отношении Получающей стороны какие-либо действия на предмет раскрытия переданной конфиденциальной информации, Получающая сторона в течение 24 часов с момента, когда ей стало известно об этих действиях, обязуется уведомить об этом Передающую сторону, а также оказать Передающей стороне содействие в предотвращении разглашения конфиденциальной информации.

2.9. Конфиденциальная информация может предоставляться уполномоченным государственным органам по их мотивированному запросу в случаях, порядке и объеме, установленном действующим законодательством Российской Федерации, с обязательным уведомлением другой стороны о таком предоставлении информации.

3. ОТВЕТСТВЕННОСТЬ СТОРОН

3.1. Получающая сторона несет ответственность за умышленное и неумышленное разглашение конфиденциальной информации, утрату документов, содержащих конфиденциальную информацию, если Получающая сторона не соблюдала столь же высокой степени осторожности, какую бы она соблюдала в разумных пределах в отношении своей собственной конфиденциальной информации аналогичной важности.

3.2. В случае установления вины Получающей стороны в разглашении конфиденциальной информации Передающая сторона имеет право на возмещение убытков, понесенных ей в связи с разглашением или использованием этой информации, в том числе расходов, понесенных в связи с судебным разбирательством.

4. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

4.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему договору, если это неисполнение явилось

следствием обстоятельств непреодолимой силы, возникших после заключения настоящего договора в результате обстоятельств чрезвычайного характера (например, землетрясения, наводнения, пожара, аварии, забастовки, войны, военных действий, революции, постановления органов государственного управления), которые стороны не могли предвидеть или предотвратить.

4.2. Сторона обязана в течение 5 (пяти) рабочих дней с момента возникновения форс-мажорных обстоятельств известить другую Сторону о невозможности исполнения обязательства. Наличие форс-мажорных обстоятельств (их возникновение и окончание) должно подтверждаться соответствующим актом, выданным уполномоченным государственным (муниципальным) органом, организацией. В случае отсутствия указанных документов Сторона не освобождается от ответственности за неисполнение (ненадлежащее исполнение) обязательств по настоящему Договору.

4.3. Если сторона не направит или несвоевременно направит извещение, предусмотренное в п. 4.2, то она обязана возместить второй стороне понесенные ею убытки.

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1. Настоящий договор вступает в силу момента подписания сторонами и действует до "___" _____ 20__ года.

5.2. Обязанности сторон сохраняют своё действие на переданную конфиденциальную информацию в течении двух лет с момента прекращения срока действия Договора.

5.3. Споры и разногласия, которые могут возникнуть из настоящего договора, стороны обязуются разрешать по возможности путем переговоров, а при не достижении согласия любая из сторон вправе обратиться за разрешением спора в арбитражный суд по месту нахождения ответчика.

5.4. Уступка права требования может быть произведена только с согласия Передающей стороны.

5.5. Внесение изменений и дополнений в настоящий Договор, а также его досрочное расторжение возможно по письменному соглашению сторон. В случае изменения юридического адреса, банковских реквизитов стороны обязаны в 7-дневный срок уведомить друг друга об этом.

5.6. Во всем, что не предусмотрено настоящим Договором, стороны руководствуются действующим законодательством Российской Федерации.

5.7. Настоящий Договор составлен в двух экземплярах по одному для каждой из сторон, имеющих одинаковую юридическую силу.

6. ЮРИДИЧЕСКИЕ АДРЕСА СТОРОН, ПЛАТЕЖНЫЕ РЕКВИЗИТЫ	
ПЕРЕДАЮЩАЯ СТОРОНА	ПОЛУЧАЮЩАЯ СТОРОНА

М.П.

М.П.

Приложение 3

Журнал «Учёт журналов»

№.п.п.	Дата начала и окончания журнала	№ журнала	Кол-во листов	Наименование журнала	Ответственное лицо Ф.И.О.	Подпись ответственного	Примечания (передача др. лицу, архив, уничтожение)
1	2	3	4	5	6	7	8

Приложение 4

Журнал «Учет носителей конфиденциальной информации»

Учетный номер и гриф конфиденци альности	Дата регистраци и	Вид (тип) носителя	Наименование информации, наносимой на носитель	Отметка о переносе информации на другой носитель или его передаче, отправлении	Отметка о возврате	Отметка об уничтожении (стирании) информации	Отметка об уничтожении носителя
1	2	3	4	5	6	7	8

Приложение 5

Журнал «Учёт подготовленных и изданных конфиденциальных документов»

Учётный номер и гриф конфиденциальности документа	Дата документа	Вид и заголовок документа	ФИО исполнителя	Количество экземпляров документа	Количество листов	
					основного документа	приложения
1	2	3	4	5	6	7

Отметка об уничтожении проектов или лиших экземпляров документа	Куда отправлен документ	Номера экземпляров	Отметка о месте нахождения документа и роспись	Примечание	
				Номер по учёту документов выделенного хранения, количество экземпляров	
8	9	10	11	12	13

Приложение 6

Журнал «Учёт поступивших конфиденциальных документов»

Учётный номер и гриф конфиденциальности документа	Дата поступления	Откуда поступил	Вид и заголовков документа	Количество экземпляров	Количество листов	
					основного документа	приложенный
1	2	3	4	5	6	7

Кому выдан документ	Подпись за получение и дата	Подпись за возврат и дата	Местонахождение документа (номер дела, листов, уничтожен по акту)	Примечание
8	9	10	11	12

Лист ознакомления с конфиденциальными документами

№ п/п	Учетный номер документа	Наименование документа	Дата ознакомления	Должность	Ф.И.О.	Подпись
1	2	3	4	5	6	7

Карточка-заместитель конфиденциального документа
рег. № _____ от «___» _____ 20__ г.

[illegible]

Приложение 9

Реестр № _____

на отправляемую корреспонденцию

Отправитель

ООО «Эн+ Диджитал»

Дата отправления

" _____ " _____ 20__ г.

№ п/п	КУДА адресован (пункт назначения)	КОМУ (подробное наименование адресата)	Регистрационный номер

№ п/п	КУДА адресован(пункт назначения)	КОМУ (подробноенаименование адресата)	Регистрационный номер

Итого: _____ пакетов (документов)

Подпись
отправителя

По настоящему реестру принято

пакетов
(документов)

" _____ " _____ 20__ г.

Подпись приемщика

Шаблон акта о выделении документов на уничтожение.

АКТ

№ _____
(дата)

(место составления)

о выделении к уничтожению документов,
не подлежащих хранению

Экспертная комиссия в составе:

- председатель комиссии – специалист ОДОУ А.Л. Иванова;
- члены комиссии - главный бухгалтер О.В. Борисова;
- специалист по ИБ С.В. Попов;
- секретарь М.И. Петрова,

составила настоящий акт о том, что в результате проведенной экспертной оценки подлежат уничтожению следующие документы, срок хранения которых истек (опись прилагается):

1. Кассовые документы за 2006 год (1 папка).
2. Авансовые отчеты за 2006 год (1 папка).
3. Кассовая книга за 2006 год.
4. Журнал регистрации расходных и приходных кассовых ордеров за 2006 год.
5. Банковские документы за 2006 год (1 папка).

Председатель комиссии
Члены комиссии:

Иванова
Борисова
Попов
Петрова

/А.Л. Иванова/
/О.В. Борисова/
/С.В. Попов/
/М.И. Петрова/

Лист регистрации изменений

Порядковый номер изменения	Основание ¹	Срок введения изменения	Изменения внес			Примечания
			ФИО	Подпись	Дата внесения изменения	

¹ Ссылка на документ, разрешающий внесение изменений и содержащий тест изменений.