АО "Мерлион"
ОГРН 1245000123720| ИНН 5024248232 | КПП 502401001
143401, Московская область, г.о. Красногорск, б-р Строителей 4, корпус 1
Тел.: +7 495 230 80 55 aomerlion@merlion.ru

ПРИКАЗ

18 апреля 2025 г. г. Красногорск № АМ-П-2

Об утверждении
Положения о коммерческой тайне и конфиденциальной информации

В целях обеспечения соблюдения установленных режимов коммерческой тайны и конфиденциальной информации, дальнейшего совершенствования систем защиты информационных ресурсов,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение о коммерческой тайне и конфиденциальной информации АО «Мерлион» (Приложение № 1 к приказу).

2. Рекомендовать дочерним обществам присоединиться к Положению о коммерческой тайне и конфиденциальной информации АО «Мерлион».

3. Опубликовать Положение о коммерческой тайне и конфиденциальной информации АО «Мерлион» на сайте https://merlion.com.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Приложение № 1: Положение о коммерческой тайне и конфиденциальной информации АО «Мерлион»

Генеральный директор А.А. Варавин

Акционерное общество «Мерлион»
(АО «Мерлион»)

Приложение № 1
к приказу Генерального директора
№ АМ-П-2 от 18. 04.2025г.

ПОЛОЖЕНИЕ
О КОММЕРЧЕСКОЙ ТАЙНЕ И КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Настоящее Положение о защите конфиденциальной информации и сведений составляющих коммерческую тайну (далее – «Положение») регламентирует вопросы, связанные с обращением конфиденциальной информации в деятельности АО «Мерлион» (далее – Компания) и дочерних Обществ Компании, присоединившихся к Положению (далее – ДО), устанавливает порядок обращения с конфиденциальной информацией и определяет основные меры ее защиты.
1.2. Положение разработано с целью защиты интересов Компании, предотвращения нанесения ущерба экономической безопасности Компании вследствие неправомерного использования конфиденциальной информации.
1.3. Положение разработано в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 29.07.2004 № 98 - ФЗ «О коммерческой тайне», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», а также иными нормативными правовыми актами, регламентирующими обращение информации, в том числе ограниченного доступа.
1.4. Требования Положения обязательны для исполнения всеми работниками Компании.
1.5. Руководители структурных подразделений Компании (управлений, отделов) несут персональную ответственность за обеспечение режима коммерческой тайны на участке деятельности подразделения.
1.6. В вопросах сохранения конфиденциальных сведений, в том числе коммерческой тайны, предоставляемых Компании контрагентами, следует руководствоваться действующим законодательством РФ, настоящим Положением, а также условиями обеспечения охраны конфиденциальности, изложенными в соответствующих договорах/соглашениях, заключенных с контрагентами.

2. ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ПОЛОЖЕНИИ.

2.1. **Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
2.2. **Конфиденциальная информация** - общее понятие, включающее в себя информацию (коммерческую тайну, персональные данные, информацию в отношении которой Компания приняла на себя обязательства перед третьими лицами по сохранению ее конфиденциальности и др.), в отношении которой обладателем предпринимаются меры по охране ее конфиденциальности.

Информация, которая может свободно распространяться в силу закона или договора, в том числе является общедоступной или подлежащей обязательному раскрытию, не рассматривается в качестве конфиденциальной.

2.3. **Коммерческая тайна** - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду либо нанести вред Компании.

Режим коммерческой тайны не устанавливается в отношений сведений, которые в силу закона не могут признаваться коммерческой тайной.

2.4. **Информация, составляющая коммерческую тайну** - сведения любого характера производственные, технические, экономические, организационные и другие, 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 коммерческой тайны.

2.5. **Обладатель информации, конфиденциального характера** - лицо, которое владеет конфиденциальной информацией, на законном основании, взявшее на себя обязательства по ограничению доступа к этой информации и обеспечению ее конфиденциальности.

2.6. **Доступ к конфиденциальной информации**, - ознакомление определенных лиц с конфиденциальной информацией, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

2.7. **Передача (предоставление) конфиденциальной информации –** передача (предоставление) информации, составляющей коммерческую тайну и/или иной конфиденциальной информации, размещенной на материальном или цифровом носителе (в том числе по техническим каналам связи), ее обладателем контрагенту на основании договора (соглашения) (в объеме и на условиях, которые предусмотрены договором, соглашением), работникам Компании в процессе исполнения ими обязанностей, предусмотренных трудовым договором, а также органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций, включая условие о принятии получателями установленных мер по охране ее конфиденциальности.

2.8. **Разглашение конфиденциальной информации**, - действие или бездействие, в результате которых информация, являющаяся конфиденциальной, 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 заключенным соглашениям и требованиям действующего законодательства.

2.9. **ИБ -** подразделение информационной безопасности.

2.10. **Структурное подразделение** - управление, отдел.

3. КАТЕГОРИИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПОРЯДОК ОТНЕСЕНИЯ СВЕДЕНИЙ К КОНФИДЕНЦИАЛЬНЫМ.

3.1. Конфиденциальная информация, обращаемая в документообороте Компании, в том числе обрабатываемая в сфере информационных технологий, в зависимости от ее значимости и возможных последствий при ее неправомерном использовании делится на две категории.

3.1.1. Первая категория - «Коммерческая тайна» - информация (сведения), разглашение (утечка) которой может привести к нарушению экономической безопасности Компании, существенно повлиять на положение на рынке, прибыль, привести к срыву реализации стратегических планов, вызвать осложнения в каких – либо направлениях деятельности, снизить эффективность работы с контрагентами, создать угрозу безопасности имуществу, персоналу, привести к дополнительным материальным затратам.

Документированной информации, которая относится к указанной категории, присваивается ограничительный гриф «Коммерческая тайна» с указанием обладателя коммерческой тайны (полное наименование и местонахождения).

3.1.2. Вторая категория – иная конфиденциальная информация, которая не может быть отнесена к коммерческой тайне, но не должна быть общедоступной, в силу возможности причинения ущерба интересам Компании или доступ к которой должен быть ограничен в соответствии с действующим законодательством РФ либо договорами/соглашениями с ее правообладателями.

Документированной информации, которая относится к указанной категории, присваивается ограничительный гриф «Конфиденциально».

Проставление ограничительного грифа «Конфиденциально» осуществляется на исходящих документах, направляемых в адрес третьих лиц.

На документах, указанных в п. 2.1.2 Перечня сведений, составляющих коммерческую тайну и иных конфиденциальных сведений (далее – Перечень), который является Приложением №1 к Положению и документах, конфиденциальность которых определена законом и порядок обращения, учета, хранения с

которыми определяется специальными нормами законодательства, ограничительный гриф «Конфиденциально» не проставляется.

3.2. Отнесение информации к конфиденциальной с присвоением соответствующей категории производится:

3.2.1. В отношении информации, собственником которой является Компания в соответствии с Перечнем.

3.2.2. В отношении информации, собственниками которой являются другие юридические и физические лица, - в соответствии с договорами/соглашениями с правообладателями этой информации.

3.3. Если сведения не включены в Перечень, но, по мнению руководителя структурного подразделения должны быть отнесены к коммерческой тайне, он предоставляет аргументированные предложения Генеральному директору Компании о включении таких сведений в Перечень.

3.4. Снижение категории ограничительного грифа, исключение сведений из Перечня и снятие ограничений на распространение сведений составляющих коммерческую тайну и иных конфиденциальных сведений осуществляются по решению Генерального директора на основании обоснованного заключения руководителя структурного подразделения, являющегося владельцем сведений.

3.5. Сведения, содержащие коммерческую тайну утрачивают необходимость защиты:

3.5.1. после исключения из Перечня;

3.5.2. по соглашению сторон, установивших ограничения;

3.5.3. По решению Генерального директора в иных случаях.

4. ПОРЯДОК ДОПУСКА РАБОТНИКОВ К СВЕДЕНИЯМ, СОСТАВЛЯЮЩИМ КОММЕРЧЕСКУЮ ТАЙНУ И ПРЕКРАЩЕНИЯ ДОПУСКА.

4.1. Основанием для допуска работников к сведениям, составляющим коммерческую тайну, является заключение трудового договора.

4.2. После заключения трудового договора сотрудник управления персоналом знакомит работника под роспись с Положением. Листы ознакомления с Положением хранятся в личном деле сотрудника.

4.3. Документы Компании, содержащие информацию, составляющую коммерческую тайну предоставляются работнику Компании, после подписания им обязательства, подтверждающего, что он предупрежден о конфиденциальности получаемой информации и об обязанности ее охранять по форме Приложения 2 к настоящему Положению, за исключением случаев, когда соответствующее условие содержится в трудовом договоре с работником.

4.4. Организация доступа работников к информационным ресурсам осуществляется руководителемструктурного подразделения в котором работает работник с соблюдением Правил по обеспечению информационной безопасности Компании (Приложение 3).

4.5. Основанием для прекращения доступа к сведениям, составляющим коммерческую тайну являются:

4.5.1. Прекращение трудовых отношений с работником. Необходимость и объем работы с конфиденциальными документами в период, когда стало известно о предстоящем прекращении трудовых отношений до момента их прекращения определяет непосредственный руководитель работника;

4.5.2. нарушение работником взятых работником на себя обязательств по неразглашению коммерческой тайны;

4.5.3. решение Генерального директора об отстранении работника от работы со сведениями составляющую коммерческую тайну. Решение принимается на основании соответствующего ходатайства руководителя структурного подразделения в котором работник работает, оформляется приказом и доводится до работника под роспись.

4.6. Документы на материальных носителях, содержащие коммерческую тайну и/или иные конфиденциальные сведения, которые находятся в работе у сотрудника, доступ которого к сведениям, составляющим коммерческую тайну и/или иные конфиденциальные сведения прекращен, должны быть незамедлительно переданы работником непосредственному руководителю, который далее их распределяет и инициирует внесение необходимых изменений в информационные системы для прекращения доступа такого работника к информационным ресурсам.

4.7. При прекращении трудовых отношений с работником за допущенные нарушения трудовой дисциплины, а также по основаниям , предусмотренных законом, по которым согласие работника не требуется, руководитель структурного подразделения, в котором работает работник (или руководитель управления персоналом) незамедлительно информируют об этом ИТ и ИБ подразделения для принятия мер по ограничению доступа работника к информационным ресурсам содержащим коммерческую тайну.

5. ОБЯЗАННОСТИ РАБОТНИКОВ ПО СОБЛЮДЕНИЮ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ.

5.1. Работники, допущенные к коммерческой тайне либо иной конфиденциальной информации, несут ответственность за соблюдение установленного режима конфиденциальности.

5.2. Работники Компании, допущенные к информации, составляющей коммерческую тайну, обязаны:

5.2.1. Не разглашать коммерческую тайну и иную конфиденциальную информацию, полученную при выполнении трудовых обязанностей в течение всего срока действия трудового договора и в течение 3 (трех) лет после его прекращения (иной срок может быть установлен отдельным соглашением);

5.2.2. Соблюдать принятые в Компании Правила информационной безопасности (Приложение 3), правила работы с документами, порядок их учета, хранения и уничтожения, доступа и работы с персональными компьютерами и иной электронной техникой Компании;

5.2.3. Знакомиться только с теми документами и информацией, содержащими коммерческую тайну и/или иные конфиденциальные сведения, к которым получили доступ в силу своих должностных обязанностей;

5.2.4. Во время работы с документами принимать меры к исключению возможности ознакомления с ними других лиц. Определять количество экземпляров документов в строгом соответствии с действительной служебной необходимостью и не допускать рассылки их адресатам, к которым они не имеют отношения;

5.2.5. В нерабочее время, а также при кратковременном отсутствии на рабочем месте не оставлять в открытом доступе документы и съемные электронные носители информации, содержащие коммерческую тайну и/или иные сведения конфиденциального характера;

5.2.6. Пресекать действия других лиц, которые могут привести к разглашению сведений составляющих коммерческую тайну. Незамедлительно информировать руководителя структурного подразделения (своего непосредственного руководителя) о наличии необоснованного интереса к сведениям, составляющим коммерческую тайну, со стороны лиц, не имеющих прямого отношения к работе с такими сведениями;

5.2.7. Документы, содержащие коммерческую тайну и находящиеся в работе на материальных носителях, хранить в отдельной папке /в специально отведенном для этого в структурном подразделении месте;

5.2.8. Перед уходом в отпуск, отъездом в служебную командировку, при переводе, увольнении сдать документы, содержащие коммерческую тайну, иные конфиденциальные сведения, на материальных носителях руководителю структурного подразделения;

5.2.9. Выполнять требования приказов и локальных нормативных актов Компании, регламентирующих сохранность коммерческой тайны;

5.2.10. Незамедлительно сообщать непосредственному руководителю, ИБ Компании об утрате или недостаче носителей информации, содержащих коммерческую тайну, пропусков, ключей от помещений, хранилищ, сейфов и о других фактах, которые могут привести к раскрытию коммерческой тайны Компании, а также о причинах и условиях возникновения таких обстоятельств;

5.3. Работникам Компании, допущенным к информации, составляющей коммерческую тайну и/или к иной конфиденциальной информации, запрещается:

5.3.1. Сообщать устно или письменно кому бы то ни было сведения, составляющие коммерческую тайну Компании, если это не связано с исполнением трудовых обязанностей;

5.3.2. Совершать действия, запрещенные Правилами информационной безопасности (Приложение 3).

5.4. Руководители структурных подразделений Компании являются ответственными за обеспечение режима коммерческой тайны на участке деятельности подразделения:

5.4.1. организуют выполнение установленных Положением режимных требований;

5.4.2. принимают меры по максимальному ограничению возможности ознакомления с информацией работников, которым по роду выполняемых ими должностных обязанностей она не требуется,

5.4.3. организуют и обеспечивают хранение документов и съемных электронных носителей информации, содержащих коммерческую тайну и иною конфиденциальную информации в сейфах или запирающихся шкафах в месте нахождения подразделения;

5.4.4. организуют и обеспечивают ведение учета лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана.

6. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ТРЕТЬИМ ЛИЦАМ.

6.1. Предоставление информации, составляющей коммерческую тайну Компании и/или иных сведений конфиденциального характера органам государственной власти, иным государственным органам, органам местного самоуправления осуществляется в порядке сроки, предусмотренные действующим законодательством РФ на основании мотивированного запроса, подписанного уполномоченным должностным лицом.

6.2. Передача информации третьими лицам, с которыми у компании имеются договорные отношения осуществляется на основании договора/соглашения в объеме и на условиях, которые предусмотрены договором/соглашением.

6.3. Предоставление конфиденциальной информации Компании третьим лицам, не являющихся стороной договора, заключенного с Компанией осуществляется по запросу руководителя заинтересованного структурного подразделения исключительно при наличии согласования отдела экономической безопасности либо Генерального директора.

6.4. Передача третьим лицам информации, составляющих конфиденциальную информации контрагентов Компании, осуществляется в соответствии с условиями договоров/соглашений с контрагентами, при наличии их согласия, за исключением случаев, когда такая передача прямо разрешена условиями договора/соглашения с контрагентом либо обязанность ее предоставления предусмотрена действующим законодательством РФ.

6.5. В случаях, когда подлежащие передаче документы содержат коммерческую тайну или иную конфиденциальную информацию, обязательно проставление на них соответствующего ограничительного грифа, в соответствии с п. 3.1.1., п. 3.1.2 Положения.

6.6. Обязанность по проставлению соответствующего ограничительного грифа на документах на бумажном носителе возлагается на отдел делопроизводства, по ходатайству руководителя заинтересованного структурного подразделения.

Обязанность по проставлению соответствующего ограничительного грифа в соответствии с п.п. 3.1.1., 3.1.2. Положения при подготовке электронных документов в правом верхнем углу первого экранного листа возлагается на сотрудника, создающего документ по согласованию с непосредственным руководителем. Возможность проставления грифа, в указанном случае должна быть технически предусмотрена программным обеспечением , которое использует сотрудник.

6.7. Входящие и исходящие конфиденциальные документы, регистрируются в журналах исходящей/входящей корреспонденции с указанием присвоенного ограничительного грифа, отдельно от учета другой документации.

6.8. Передача и предоставление документов, содержащих коммерческую тайну и/или иную конфиденциальную информацию, должны осуществляется способом исключающим возможность ознакомления с ними третьих лиц , с составлением документов, подтверждающих факт их получения адресатом.

7. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ И/ИЛИ ИНЫХ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА.

7.1. Разглашение сведений и утрата документов, составляющих коммерческую тайну и/или иной конфиденциальной информации, нарушение режима защиты коммерческой тайны и конфиденциальной информации, относится к нарушению трудовых обязанностей.
7.2. Работник Компании, своими действиями или бездействиями нарушивший, или допустивший нарушение режима работы с конфиденциальной информацией и информацией, составляющей коммерческую тайну и иную конфиденциальную информацию несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации. Также возможно привлечение к гражданско-правовой, административной, уголовной ответственности в соответствии с действующим законодательством.

8. ПОРЯДОК ПРИСОЕДИНЕНИЯ ДОЧЕРНИХ ОБЩЕСТВ.

8.1. Присоединение ДО к настоящему Положению и/или изменениям к нему осуществляется путем принятия соответствующего решения органом управления ДО, имеющим необходимые полномочия согласно нормам законодательства РФ и учредительных документов.
8.2. ДО в течение 5 (пяти) рабочих дней с даты принятия решения о присоединении к Антикоррупционной политики и/или к каждому изменению направляет уведомление и копию соответствующего решения органа управления в АО «Мерлион».
8.3. Положение подлежит опубликованию на официальном сайте Компании. Перечень ДО, присоединившихся к настоящему Положению, также размещается на указанном сайте и подлежит обновлению по факту изменений.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Положение вступает в силу с момента его утверждения генеральным директором Компании.
9.2. Изменения и дополнения в Положение вносятся на основании приказа генерального директора Компании.
9.3. Если в результате изменения законодательства Российской Федерации отдельные пункты Положения вступают в противоречие с законодательством, указанные пункты Положения утрачивают силу, и до момента внесения изменений и дополнений в Положение применяются нормы законодательства Российской Федерации.

10. ПРИЛОЖЕНИЯ

10.1. Перечень сведений, составляющих коммерческую тайну и иных конфиденциальных сведений.
10.2. Обязательство о неразглашении коммерческой тайны.
10.3. Правила информационной безопасности.
10.4. Форма журнала учета лиц, допущенных к коммерческой тайне.

Приложение № 1
к Положению о коммерческой тайне и
конфиденциальной информации

ПЕРЕЧЕНЬ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ И ИНЫХ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ.

1. ПЕРЕЧЕНЬ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ

1.1. Информация о финансовых показателях Компании, показатели рентабельности, прибыли и убытков.
1.2. Налоговая, статистическая, управленческая отчетность по результатам деятельности Компании. Совокупные аналитические данные, сводные данные учетных документов.
1.3. Сведения о размерах и условиях кредитования Компании. Информация об оборотах по банковским счетам.
1.4. Сведения о кредиторской, дебиторской задолженности, а также об иных долговых обязательствах Компании (за исключением сведений, о задолженности Компании по выплате заработной платы и социальным выплатам);
1.5. Стратегические планы, планируемые бюджеты, инвестиционные проекты Компании.
1.6. Сведения о структуре стоимости (себестоимости) товаров, производимой продукции и услуг (работ) Компании, за исключением случаев предусмотренных законодательством РФ.
1.7. Любые данные из управленческого учета и личных кабинетов маркетплейсов. Сведения о запасах товаров, материалов, комплектующих, готовой продукции и другого имущества Компании. Данные об объемах перевозок, транзита грузов, операционных расходах.
1.8 Результаты маркетинговых исследований, применяемые маркетинговые инструменты. Информация о планируемых маркетинговых акциях, рекламных компаниях, специальных ценах, потенциальных сделках.
1.9. Информация о планируемых сделках консолидации компаний или активов компаний (M&A) , в том числе информация о состоянии переговоров, достигнутых договоренностях, содержание и условия документов, которыми обмениваются стороны в рамках таких переговоров, включая проектные соглашения, финансовые и юридические оценки, подробности предложений и откликов сторон, сведения о текущем статусе переговорного процесса и стратегических интересах участников сделки.
1.10. Сведения о клиентах, поставщиках, подрядчиках и иных контрагентах, а также результатах переговоров с контрагентами (партнерами) Компании и условиях сотрудничества с ними.
1.11. Информация о логистических цепочках и маршрутах доставки.
1.12. Сведения, составляющие коммерческую тайну контрагентов (партнеров) Компании.
1.13. Сведения о применяемых оригинальных методах управления Компанией, системах планирования и контроля. Сведения о количестве и структуре подразделений Компании, схеме и методах их взаимодействия и управления. Планируемые организационные и структурные изменения внутри Компании.
1.14. Информация об объектах интеллектуальной собственности до получения ими правовой охраны / защиты.
1.15. Служебные произведения Общества: задания на разработку, результаты работ - все, что относится к создаваемым объектам интеллектуальной собственности.
1.16. Информация о планируемых разработках или модернизациях технологий и процессов, позволяющих повысить конкурентоспособность Компании на внутреннем и внешнем рынке.
1.17. Сведения о порядке и состоянии организации безопасности и системе охраны, пропускном режиме, систем охранной сигнализации и т.п.

1.18. Сведения об информационных технологиях, программном и технологическом обеспечении, конфигурации программно- аппаратных комплексов, области применении (наименование, описание и назначение).

1.19. Сведения о применяемых в Компании технических или программных средствах информационной безопасности (наименование, архитектура, область действия), средствах защиты информации и обеспечения доступа к информации и информационным ресурсам Компании.

1.20. Материалы и результаты внешних аудиторских проверок Компании.

1.21. Сведения о подготовке к участию в конкурсах, тендерах или аукционах.

1.22. Положения, регулирующие порядок создания и исполнения заказов на продажу (покупку), относящихся к коммерческой деятельности Компании.

1.23. Информация о трудовой, производственной, финансовой эффективности работников и подразделений компании.

1.24. Информация о кадровом резерве;

1.25. Сведения о характеристике работника(ов), составленной руководством, службой по работе с персоналом, иными подразделениями и службами для внутреннего использования

1.26. Основные показатели и метрики HR-аналитики, включая сведения о текучести кадров, оценке уровня вовлеченности, численности работников по подразделениям, содержании и результатах тестирования, опросов.

2. ПЕРЕЧЕНЬ ИНЫХ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ.

2.1. К сведениям, которые не составляют коммерческую тайну Компании, но носят конфиденциальный характер, относятся:

- сведения о результатах совещаний, составе участников при условии, что до начала совещания или во время проведения совещания было сделано предупреждение в любой форме о конфиденциальности такого совещания;
- платежные документы;
- сведения об исчисления в уплате налогов и обязательных платежей;
- о численности и составе работников;
- о системе и структуре оплаты труда и вознаграждений, включая премий, бонусы, надбавки, доплаты и т.д.;
- служебные сведения, доступ к которым ограничен органами государственной власти;
- информация об идентификационных данных (логин, пароль) для доступа к информационным системам и иным хранилищам информации, доступ к которым ограничен (помимо прочего - к личным кабинетам Компании на сторонних ресурсах) – данные корпоративной учетной записи и учетной записи для сторонних информационных ресурсов, а также о ключах электронной подписи (проверочные смс-коды и пр.), об идентификационных данных к банк-клиенту;
- сведения о порядке и датах внутренних проверок в Компании.

2.2. Конфиденциальные сведения, защищаемые государством в иных режимах:

- персональные данные;
- сведения, связанные с профессиональной деятельностью, доступ к которой ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, тайна переписки и телефонных переговоров, почтовых отправлений, телеграфных сообщений и т.д.);
- сведения «Для служебного пользования" (ДСП);
- сведения составляющие государственную тайну;
- сведения, защищаемые нормами права интеллектуальной собственности и иного специального законодательства.

Приложение №2
к Положению о коммерческой тайне и
конфиденциальной информации

ОБЯЗАТЕЛЬСТВО
о неразглашении коммерческой тайны

Я_____
(фамилия, имя, отчество)

в качестве работника компании ____ "_____" (далее - «Компания») в период трудовых отношений и в течение 3 (трех) лет после их окончания, в соответствии с трудовым договором, заключенным между мной и Компанией, а также соответствующих положений по обеспечению сохранности коммерческой тайны,

обязуюсь:

1) не разглашать сведения, составляющие коммерческую тайну Компании (согласно перечня сведений, составляющих коммерческую тайну Компании), которые мне будут доверены или станут известны в рамках исполнения должностных обязанностей;
2) выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению сохранности коммерческой тайны Компании;
3) в случае попытки посторонних лиц получить от меня сведения о коммерческой тайне Компании немедленно сообщить уполномоченным должностным лицам, и\или непосредственному начальнику;
4) сохранять коммерческую тайну контрагентов (партнеров) Компании;
5) не использовать знание коммерческой тайны Компании для занятий любой деятельностью, которая в качестве конкурентного действия может нанести ущерб Компании;
6) в случае моего увольнения, все носители коммерческой тайны Компании (не зависимо от способа их представления, например, материальные или электронные), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в Компании, передать уполномоченному должностному лицу либо непосредственному руководителю;
7) об утрате или недостаче носителей коммерческой тайны, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению коммерческой тайны Компании, а также о причинах и условиях возможной утечки сведений немедленно сообщать уполномоченным должностным лицам или непосредственному руководителю.

Я предупрежден, что в случае невыполнения любого из пунктов настоящего обязательства трудовые отношения со мной могу быть расторгнуты в соответствии с пп. в п. 6 ч.1. ст. 81 ТК РФ.

Подтверждаю, что до моего сведения доведены с разъяснениями соответствующие Положения по обеспечению сохранности коммерческой тайны Компании.

Мне известно, что нарушение положений, направленных на обеспечение охраны и конфиденциальности коммерческой тайны, может повлечь привлечение к уголовной, административной, гражданско-правовой или иной ответственности, предусмотренной действующим законодательством Российской Федерации.

_____/_____
(Подпись / расшифровка подписи)

(Дата)

Приложение №3
к Положению о коммерческой тайне и
конфиденциальной информации

Правила информационной безопасности

1. Общие принципы

1.1. Каждый работник Компании, а также партнер или представитель партнера, который получает доступ в информационные системы Компании, обязан ознакомиться с настоящими Правилами информационной безопасности (далее Правила) и исполнять их.

1.2. Отказ от ознакомления и согласия с правилами может стать основанием для блокировки пользователя в информационных системах Компании.

1.3. Несоблюдение настоящих Правил может быть основанием для применения меры дисциплинарного воздействия (вплоть до увольнения) к работнику или расторжения договорных отношений с партнерами.

1.4. Руководители подразделений несут персональную ответственность в части доведения до подчиненных содержания настоящих Правил и организации работы подразделения в соответствии с настоящими Правилами.

1.5. Любые служебные вопросы, вступающие в противоречие с настоящими Правилами, должны согласовываться с Управлением ИБ.

1.6. Если согласованное Управлением ИБ решение вступает в противоречие с некоторыми пунктами настоящих Правил, то согласованное решение имеет более высокий приоритет.

1.7. Если работнику Компании становится известно о совершении кем-либо действий, нарушающих настоящие Правила или планировании таких действий, работник обязан незамедлительно сообщить об этом в Управление Информационной Безопасности по адресу isd@merlion.ru.

2. Термины и определения

2.1. Локальная сеть – проводная или беспроводная компьютерная сеть Компании (за исключением гостевых сетей), включающая в себя вычислительные устройства (маршрутизаторы, коммутаторы, точки доступа, компьютеры, серверы, принтеры и другие устройства) и технологии, необходимые для обеспечения обмена данными между этими устройствами.

2.2. Служебный компьютер (далее компьютер) – стационарный, переносной или виртуальный компьютер, принадлежащий Компании, подключенный либо не подключенный к локальной сети Компании, на котором организовано либо не организовано рабочее пространство.

2.3. Периферийное оборудование – различные устройства ввода-вывода или отображения информации, такие, как: мониторы, клавиатуры, мыши, принтеры, сканеры и другие аналогичные устройства. К периферийным устройствам в контексте данного документа не относятся устройства хранения информации, подключаемые через внешние интерфейсы компьютера: USB, eSATA и т.п.

2.4. Служебная информация – не опубликованная Компанией в открытых источниках информация, относящаяся к деятельности Компании или деятельности ее партнеров, доступная всем работникам Компании, партнерам или представителям партнера и свободно передаваемая внутри информационных систем Компании.

2.5. Коммерческая тайна – не опубликованная Компанией в открытых источниках информация, относящаяся к ее деятельности или деятельности партнеров, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, защищаемая ФЗ «О коммерческой тайне» № 98-ФЗ от 29.07.2004 и определяемая внутренним нормативным документом – Положением о коммерческой тайне и конфиденциальной информации Компании.

2.6. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
2.7. Конфиденциальная информация – информация из п 2.5.– 2.6. настоящих Правил, а также иная, определяемая внутренним нормативным документом – «Положением о коммерческой тайне и конфиденциальной информации» Компании.
2.8. Информационный ресурс – информационный массив данных или объект с информацией, обрабатываемый в информационной системе Компании.
2.9. Информационная система – совокупность технических средств, позволяющая вводить, выводить, обрабатывать и хранить информацию.
2.10. Учетная запись – хранимая в информационной системе совокупность данных о пользователе (в частности, логин и пароль), необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и рабочему пространству.
2.11. Партнер – юридическое или физическое лицо, состоящее в договорных отношениях с Компанией.
2.12. Пользователь – работник Компании, партнер или представитель партнера, получивший на основании договорных обязательств доступ к информационным системам Компании и работающий в них с использованием персональной или обезличенной учетной записи.
2.13. Рабочее пространство – совокупность доступов ко всем необходимым информационным ресурсам и приложениям Компании (почте, сетевым каталогам, корпоративным системам и т.д.), организованная посредством расположенного в локальной сети Компании стационарного или виртуального компьютера (в т.ч. удаленного).
2.14. Корпоративный электронный адрес – общий или персональный адрес ящика электронной почты, зарегистрированной в одном из принадлежащих Компании домене.
2.15. Некорпоративный электронный адрес – адрес ящика электронной почты любого стороннего домена, не принадлежащего Компании (mail.ru, yandex.ru, gmail.com и т.д.).
2.16. Корпоративный доступ в Интернет – доступ, предоставленный для выполнения служебных обязанностей, использующий вычислительные ресурсы Компании для взаимодействия с глобальной сетью Интернет.
2.17. Корпоративная VPN – виртуальная сеть, построенная с использованием вычислительных ресурсов и аппаратно-программных средств Компании, позволяющая обеспечить доступ к рабочему пространству и корпоративным ресурсам Компании через Интернет. Корпоративная VPN подпадает под те же правила, что и локальная сеть.

3. Правила настройки компьютеров и рабочего пространства

3.1. Установку, подключение, настройку, изменение конфигурации компьютеров и организацию доступа к рабочему пространству осуществляют сотрудники технической поддержки либо сотрудники, на которых возложена такая обязанность. Самостоятельно подключать, настраивать, изменять конфигурацию, вскрывать и перемещать компьютеры или периферийное оборудование разрешено только по согласованию со службой технической поддержки.
3.2. Локальные диски переносных компьютеров должны быть зашифрованы методом полного шифрования диска.
3.3. Запрещено ограничивать доступ к компьютеру сотрудникам службы технической поддержки или сотрудникам службы информационной безопасности.
3.4. Запрещено организовывать и предоставлять доступ к своему рабочему пространству другим пользователям. В случае необходимости предоставления доступа внешним службам поддержки или партнерам, требуется согласование с Управлением ИБ.
3.5. Запрещено подключать к локальной сети Компании личные устройства.
3.6. Запрещено подключать напрямую к локальной сети Компании корпоративные мобильные устройства, предназначенные для удаленной работы (в частности, служебные ноутбуки).

Подключение таких устройств к локальной сети компании должно осуществляться исключительно через корпоративную VPN.

4. Правила использования ПО

4.1. На компьютерах Компании установлено антивирусное программное обеспечение. Запрещено пытаться отключать или обходить средства защиты без согласования со службой ИБ.

4.2. Пользователю запрещено самостоятельно скачивать, устанавливать и запускать на компьютерах Компании любое программное обеспечение (далее ПО), если это не входит в его должностные обязанности.

4.3. Установка любого ПО выполняется специалистами службы технической поддержки по согласованию со службой ИБ. Все скачанное ПО подлежит проверке штатным АВПО.

4.4. Запрещается преднамеренная установка, распространение или использование вредоносного программного обеспечения (включая вирусы, трояны, шпионские программы, программы-вымогатели, кейлоггеры, боты и иные формы вредоносного кода) на любых устройствах, подключенных к корпоративной сети, а также на личных устройствах, используемых для работы с корпоративными данными.

4.5. При обнаружении признаков заражения (несанкционированные действия системы, подозрительные процессы, всплывающие окна с требованиями выплат и т.п.) следует немедленно сообщить в Управление ИБ isd@merlion.ru и выключить устройство или отключить его от сети.

5. Правила использования внешних устройств и носителей информации

5.1. Разрешено подключать к компьютерам только следующие устройства: принтер, сканер, web-камера, аудио-гарнитура, клавиатура, мышь.

5.2. Подключение устройств может производиться через физические интерфейсы (USB, SD и др), либо беспроводным способом. Беспроводные протоколы подключения устройств не должны поддерживать передачу файлов.

5.3. Возможность подключения других устройств и внешних носителей информации (флеш накопителей, внешних жестких дисков и т.д.) требуется согласовывать со службой ИБ.

5.4. Пользователи обязаны использовать предоставленный на компьютере доступ к устройствам и носителям информации только для тех целей, которые были указаны в заявке и согласованы службой ИБ. Допускается подключение устройств для их зарядки, не требующей специального доступа.

5.5. Запрещено делиться предоставленным на компьютере доступом к устройствам и носителям информации с кем-либо.

6. Правила работы с информацией и информационными ресурсами

6.1. Для работы в информационной системе Компании или со сторонними сервисами от имени Компании пользователю предоставляется одна или несколько учетных записей. Пользователь несет личную ответственность за сохранность данных для авторизации (паролей, токенов авторизации и других средств доступа).

6.2. Запрещено сообщать пароль или передавать токен авторизации от учетной записи третьим лицам.

6.3. Запрещено оставлять носители с паролем от учетной записи в доступной для третьих лиц зоне.

6.4. Запрещено работать в информационной системе Компании под чужой учетной записью.

6.5. Запрещено предпринимать любые действия, направленные на несанкционированное повышение привилегий в системах, или получение несанкционированного доступа, включая использование уязвимостей или обход механизмов безопасности.

6.6. В случае подозрения, что данные для авторизации (пароль, приватный ключ или другие средства доступа) стали доступны кому-либо, помимо владельца учётной записи, необходимо:
6.6.1. немедленно сменить данные для авторизации самостоятельно или обратиться за помощью в службу технической поддержки.
6.6.2. незамедлительно уведомить Управление ИБ по электронной почте isd@merlion.ru
6.7. Запрещено предоставлять доступ к служебной информации и информационным ресурсам другим пользователям, у которых отсутствует подтвержденный доступ к этим ресурсам.
6.8. Запрещено предоставлять доступ к служебной информации и информационным ресурсам Компании партнерам, если это не обосновано служебной необходимостью и не является частью выполнения договорных обязательств.
6.9. Запрещено оставлять документы, содержащие служебную информацию, в принтерах, сканерах и копировальных аппаратах. Если при печати не произошло ошибки и вы не нашли документы в принтере, необходимо немедленно связаться со службой технической поддержки для поиска документа и принтера, на котором он распечатался.
6.10. Печать документов, содержащих служебную информацию, в режиме удаленной работы должна производится не для удобства работы с данными, а исключительно в случаях, когда служебные задачи подразумевают работу с бумажными носителями.

7. Правила работы с конфиденциальной информацией

7.1. Хранить и обрабатывать конфиденциальную информацию допускается исключительно в принадлежащих или контролируемых Компанией информационных системах (в т.ч. на носителях информации), а также в информационных системах партнеров, с которыми осуществляется взаимодействие в рамках исполнения договорных обязательств, с учетом оценки и контроля избыточности, критичности и сроков хранения информации.
7.2. При обработке конфиденциальной информации независимо от формы ее представления (бумажной, электронной, устной) работник обязан обеспечить ее безопасность. В частности, запрещается: копирование такой информации на некорпоративные внешние носители, отправка на адреса электронной почты в публичных доменах, размещение на неконтролируемых Компанией ресурсах, публикация в сети Интернет или иных публичных источниках, обсуждение в публичных местах и по телефону.
7.3. Запрещено передавать конфиденциальную информацию (в т.ч. между работниками Компании) посредством не контролируемых Компанией сервисов обмена информацией (whatsapp, telegram и др.)
7.4. Конфиденциальная информация является частным случаем служебной информации, т.е. на нее также распространяются правила, действующие в отношении служебной информации. Размещение, обработка и передача конфиденциальной информации должны происходить в рамках исполнения служебных задач.

8. Правила работы с корпоративной почтой и системами ВКС

8.1. Корпоративная почта и системы видеоконференций (далее ВКС) предназначены исключительно для выполнения служебных задач.
8.2. Запрещено использовать корпоративные адреса электронной почты для регистрации на сторонних ресурсах, если этого не требуется для выполнения рабочих обязанностей.
8.3. Пользователи обязаны сохранять конфиденциальность информации, передаваемой через корпоративную почту и обсуждаемой в рамках ВКС и не разглашать ее третьим лицам.
8.4. Запрещено отправлять письма, содержащие служебную информацию, с корпоративных электронных адресов на некорпоративные электронные адреса, в том числе на личные электронные адреса, за исключением случаев взаимодействия с партнером, когда данная отправка является частью исполнения договорных обязательств.

8.5. При работе с электронной почтой запрещено открывать вложения, которые могут нанести вред информационным ресурсам Компании.
8.6. Запрещено открывать гиперссылки в письмах, имеющих признаки фишинговых сообщений.
8.7. Запрещено передавать служебную информацию через ВКС, включая прикрепление файлов к приглашениям на ВКС и в процессе видеосессии, если участники не имеют подтвержденного доступа к этой информации.
8.8. Запрещено использовать ВКС для обсуждения конфиденциальной информации в местах, где не может быть обеспечена конфиденциальность обсуждения.
8.9. При организации видеоконференций, на которых обсуждаются конфиденциальные вопросы, требуется удостовериться в подлинности участников, чтобы исключить участие посторонних лиц в конференции.
8.10. При организации видеоконференций, требуется выбирать имя для конференции так, чтобы оно не раскрывало конфиденциальной информации.
8.11. Запрещается вести запись сессии ВКС любыми средствами без предварительного согласования со всеми участниками.

9. Правила работы в сети Интернет

9.1. Для работы в сети Интернет с корпоративных компьютеров разрешено использовать только браузеры, установленные и настроенные службой технической поддержки. Запрещено менять настройки браузеров, выставленные политикой безопасности.
9.2. Запрещено использовать корпоративный доступ в Интернет в целях, дискредитирующих Компанию, способных повлечь негативные для Компании последствия или негативно повлиять на репутацию Компании (в частности, необходимо избегать публикации или распространения клеветы, дезинформации, экстремистских высказываний).
9.3. Запрещено использовать неконтролируемые Компанией интернет-сервисы для хранения и обработки служебной информации, в частности, различные сервисы хранения, синхронизации и обмена файлами, создания и редактирования документов, управления задачами, расписаниями, проектами и онлайн-конверторы файлов. Любые исключения должны быть согласованы с Управлением ИБ.
9.4. Запрещено подключать компьютеры, подключенные к локальной корпоративной сети, одновременно к другим сетям, в частности, через gsm-модем, точку доступа wi-fi или внешнее VPN подключение.

10. Ответственность

10.1. За нарушение правил настоящего Документа работник Компании несет ответственность, предусмотренную Трудовым Кодексом, Кодексом об административных правонарушениях и Уголовным кодексом РФ в зависимости от степени нарушения и последствий. К нарушителю в т.ч. может быть применена мера дисциплинарного воздействия, в соответствии с Положением о применении дисциплинарных воздействий. С партнером Компании может быть разорван договор или применены другие меры, предусмотренные заключенными соглашениями.

11. Приложения

11.1. Приложение 1. Памятка о фишинге (пункт 8.6 правил) Приложение 1. Перечень разрешённого ПО (пункт 4.4 правил);
11.2. Приложение 2. Типы файлов, пересылка которых запрещена через корпоративную почту и письма с которыми блокируются на почтовом сервере (пункт 8.5 правил);
11.3. Приложение 3. Памятка о фишинге (пункт 8.6 правил).

Приложение №4
к Положению о коммерческой тайне и
конфиденциальной информации

ФОРМА

ЖУРНАЛА УЧЕТА ЛИЦ, ДОПУЩЕННЫХ К КОММЕРЧЕСКОЙ ТАЙНЕ

_____

(наименование юридического лица)

№	Ф.И.О.	Должность	Дата доступа	Основание доступа (Трудовой договор/NDA...)	Подпись руководителя структурного подразделения