УТВЕРЖДАЮ:
Генеральный директор
_____Д.Л. Мельников
«28» 10 2019 г.

ПОЛИТИКА ОТКРЫТОГО АКЦИОНЕРНОГО ОБЩЕСТВА «СОЛИКАМСКИЙ МАГНИЕВЫЙ ЗАВОД» В ОБЛАСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящая политика устанавливает обязательства, определяет порядок и намерения ОАО «СМЗ» (далее Общество) соответствовать законодательству Российской Федерации в области обработки и защиты персональных данных лиц, состоящих в трудовых, гражданско-правовых и иных отношениях (далее субъектов) с Обществом.

1.2. Назначением настоящей Политики является обеспечение необходимого и достаточного уровня информационной безопасности персональных данных субъектов, хранящихся в Обществе, от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Обработка и защита персональных данных в Обществе осуществляется в полном соответствии с законодательством Российской Федерации с целью соблюдения законных прав субъектов персональных данных на неприкосновенность частной жизни, личную и семейную тайну, а так же с целью защиты интересов Общества от нанесения ущерба посредством нецелевого использования или воздействия на персональные данные.

1.4. Общество обязано ознакомить всех работников с настоящей Политикой под личную подпись.

1.5. Управление настоящей Политикой (планирование, разработка, внесение изменений, рассылка, хранение и т.д.) осуществляются в соответствии с требованиями методологической инструкции «Документированная информация».

1.6. Настоящая Политика подлежит пересмотру и изменению в случае:

- изменения законодательства Российской Федерации,
- выявления несоответствий, затрагивающих обработку персональных данных,
- результатов проведения внутреннего аудита,
- по решению руководства Общества.

1.7. Настоящий документ обязателен к применению во всех структурных подразделениях общества и подлежит опубликованию на официальном сайте Общества в сети Интернет для обеспечения неограниченного доступа к документу различных категорий субъектов, в отношении которых Обществом осуществляется обработка персональных данных, в соответствии с требованиями действующего законодательства.

1.8. При разработке Политики использованы следующие документы:

- Конституция Российской Федерации,

- Трудовой Кодекс Российской Федерации,
- Кодекс Российской Федерации об административных правонарушениях,
- Федеральный закон от 27.07.2006г. № 152-ФЗ «О персональных данных»,
- Постановление Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований защите персональных данных при их обработке в информационных системах персональных данных»,
- Постановление Правительства Российской Федерации от 06.07.2008г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»,
- Постановление Правительства Российской Федерации от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
- Методологическая инструкция «Документированная информация».

2. Основные понятия, термины и определения, используемые в Политике

В настоящей Политике применены следующие понятия, термины и определения:

2.1. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному физическому лицу (субъекту персональных данных). К такой информации, в том числе относятся сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

2.2. **Субъект персональных данных** – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

2.3. **Общество** - открытое акционерное общество «Соликамский магниевый завод».

2.4. **Оператор** – Общество, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а так же определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.5. **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.6.**Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.7. **Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.8. **Идентификация в информационных системах** – присвоение субъектам и объектам идентификатора и сравнения идентификатора с перечнем присвоенных идентификаторов.

2.9. **Аутентификация** – процедура проверки подлинности пользователя путем сравнения введенного им пароля с паролём в базе данных пользователей.

2.10. **Конфиденциальность персональных данных** - обязательное для соблюдения Обществом требование сохранять в тайне персональные данные, хранимые, обрабатываемые и передаваемые по каналам связи. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

3. Цели обработки персональных данных

3.1. Персональные данные обрабатываются в Обществе в целях:

- защиты законных интересов субъектов персональных данных и Общества от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи,
- осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Российской Федерации, в Федеральную налоговую службы, в Фонд социального страхования Российской Федерации, в федеральный Фонд обязательного медицинского страхования, а так же в иные государственные органы,
- для регулирования трудовых отношений с работниками (содействия в трудоустройстве, обучение и продвижения по службе, обеспечение личной безопасности, контроль количества и качества выполняемой работы) и заключения, исполнения и прекращения договоров с контрагентами,
- для обеспечения пропускного и внутриобъектовоого режима в Обществе,
- для формирования справочных материалов для внутреннего информационного обеспечения деятельности Общества,
- для осуществления обработки персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с Федеральным Законом,
- в иных законных целях.
-

3.2.Для достижения поставленных целей Общество обеспечивает:

- конфиденциальность персональных данных от незаконного распространения,
- соблюдение принципов, указанных в разделе 4 данной Политики,
- целостность и достоверность персональных данных, которые хранятся и обрабатываются в информационных системах персональных данных Общества и передаются по каналам связи,

- доступность персональных данных для пользователей, которым для решения поставленных задач нужно иметь возможность в нужное время получить необходимые персональные данные.

4. Принципы и условия обработки персональных данных

4.1. Общество, являясь оператором персональных данных, осуществляет обработку персональных данных работников Общества и других субъектов персональных данных, не состоящих с Обществом в трудовых орошениях.

4.2. При определении объема и содержания персональных данных работника, Общество руководствуется законодательством Российской Федерации, Уставом Общества, настоящей Политикой, локальными актами Общества.

4.3.Обработка персональных данных в Обществе осуществляется на основе следующих принципов:

- обработка на законной основе;
- не допустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработка только тех персональных данных, которые отвечают целям их обработки;
- соответствия содержания и объема обрабатываемых персональных данных целям обработки;
- не допустимости избыточности обрабатываемых персональных данных по отношению к целям их обработки;
- обеспечения точности при обработке персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки;
- своевременности принятия мер по удалению или уточнению неполных или неточных персональных данных;
- обеспечение хранения в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или получателем по которому является субъект персональных данных;
- установления порядка уничтожения и обезличивания персональных данных, по достижении целей обработки, если иное не предусмотрено законодательством,
- не допустимости обработки специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

4.4. Условия обработки персональных данных Обществом:

- обработка персональных данных осуществляется с согласия в письменной форме субъекта персональных данных на обработку его персональных данных,

- обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством российской Федерации и оператора функций, полномочий и обязанностей,
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а так же для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем,
- обработка персональных данных необходима для осуществления прав и законных интересов Общества или третьих лиц либо достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных,
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с Федеральным Законом,
- обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах,
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

5. Субъекты персональных данных и их права

5.1. В Обществе обрабатываются персональные данные следующих категорий субъектов персональных данных:

- работники Общества,
- лица, являющиеся соискателями должностей (работы) в Обществе,
- физические лица, состоящие с Обществом в гражданско-правовых отношениях,
- физические лица, обратившиеся в Общество с запросами любого характера, и представившие в связи с этим свои персональные данные,
- представители контрагентов,
- иные категории лиц.

5.2. Обработка персональных данных субъекта возможна как с использованием средств автоматизации, так и без них.

5.3. Обществом определяется перечень обрабатываемых персональных данных, составленный в соответствии с законодательством российской Федерации и локальными нормативными актами Общества.

5.3. Субъекты персональных данных имеют право на:

- полную информацию об их персональных данных, обрабатываемых в Обществе, в том числе информацию, касающуюся обработки их персональных данных,

- доступ к своим персональным данным, включая право на получение копий любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законодательством,
- уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки,
- отзыв согласия на обработку персональных данных,
- принятие предусмотренных законом мер по защите своих прав,
- обжалование действий или бездействия Общества, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд,
- осуществление иных прав, предусмотренных законодательством Российской Федерации.

6. Обеспечение безопасности персональных данных

6.1. При обработке персональных данных Общество принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а так же от иных неправомерных действий отношении персональных данных.

6.2. Обеспечение безопасности персональных данных достигается путем:

- своевременного определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных, оценки и прогнозирования источника угроз информационной безопасности и создания механизма оперативного реагирования на угрозы,
- применения организационных и технических мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные законодательством Российской Федерации уровни защищенности персональных данных,
- применение, прошедших в установленном порядке процедуру оценки соответствия, средств защиты информации, а так же защиты системы от внедрения несанкционированных программ,
- защиты от вмешательства в процесс функционирования информационных систем Общества посторонних лиц (доступ только для зарегистрированных в установленном порядке пользователей),
- защиты от несанкционированного доступа к персональным данным (обеспечивается возможность доступа только к тем системам и выполнения только тех операций с ними,

которые необходимы конкретным пользователям для выполнения своих служебных обязанностей),

- установления правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, аутентификации пользователей, а так же обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных,
- осуществлением контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных, защиты персональных данных от утечки по техническим каналам при ее обработке, хранении и передачи по каналам связи,
- назначение лица, ответственного за организацию обработки персональных данных.

6.3. Защита персональных данных представляет собой жестко регламентированный и динамический технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности предприятия.

6.4. Защита персональных данных субъекта персональных данных от неправомерного их использования или утраты обеспечивается Обществом путем разработки и применения организационных и технических средств.

6.5. Основными объектами системы безопасности персональных данных являются:

- информационная система персональных данных;
- процессы обработки персональных данных, регламенты и процедуры;
- объекты и помещения, в которых расположены компоненты информационной системы персональных данных.

6.6. Для защиты информационной системы персональных данных в Обществе реализуются следующие меры:

6.6.1. Правовые меры защиты проявляются в принятии локальных нормативных актов и иных документов в области обработки и защиты персональных данных, регламентирующих правила обработки персональных данных с установлением прав, обязанностей и ответственности участников информационных отношений в процессе обработки. Обязательным условием документов является полнота и непротиворечивость требований организационно-распорядительных документов Общества по вопросам обеспечения безопасности информации.

6.6.2. Организационные меры защиты заключаются:

- в подготовке работников, ответственных за обеспечение безопасности обработки персональных данных, организации обучения и проведения методической работы с работниками структурных подразделений,

- в доведении до сотрудников требований нормативно-методических документов по защите информации и персональных данных,
- в осуществлении строго учета всех подлежащих защите информационных систем персональных данных (информации, каналов связи, серверов, документов),
- в осуществлении учета действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационной защиты,
- в осуществлении контроля за соблюдением требований Общества по обеспечению безопасности информации пользователями информационной системы персональных данных,
- в проведении воспитательной и разъяснительной работы с сотрудниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

6.6.3. Административные меры защиты регламентируют процесс функционирования системы обработки персональных данных, деятельность обслуживающего персонала и порядок взаимодействия пользователей с системой таким образом, чтобы исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Административные меры включают в себя:

- регламентацию доступа в помещения, где расположены информационные системы персональных данных. Для обеспечения физической сохранности находящихся в помещении защищаемых ресурсов, в том числе персональных данных, обрабатываемых без использования средств автоматизации, исключается возможность бесконтрольного проникновения в помещение посторонних лиц и несанкционированного доступа к материальным носителям персональных данных,
- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний, а так же их допуска к использованию информационной системы персональных данных. Для этого приказом генерального директора утверждается список должностей, уполномоченных на обработку персональных данных и (или) имеющих доступ к персональным данным работников. Расширение права доступа и предоставление доступа к дополнительным информационным ресурсам, в обязательном порядке, должно согласовываться с ответственными за организацию обработки персональных данных,
- регламентацию процессов обслуживания и усовершенствования программных ресурсов, когда конфигурация автоматизированных рабочих мест сотрудников, имеющих доступ к ресурсам информационной системы, соответствуют кругу возложенных на этих пользователей функциональных обязанностей. Рациональное размещение рабочих мест сотрудников способствует исключению возможности бесконтрольного использования защищаемой информации,
- организацию порядка хранения, уничтожения информации,

- ответственность работников за нарушение установленного порядка пользования ресурсами информационных систем Общества должна определяться в соответствии с требованиями действующего законодательства и локальных нормативных актов Общества.

6.6.4. Физические меры защиты предназначены для защиты доступа потенциальных нарушителей к персональным данным путем использования технических средств визуального наблюдения (видеонаблюдения), связи и охранной сигнализации. Для осуществления защиты информационной системы должен быть регламентирован порядок приема, учета и контроля деятельности посетителей, а так же осуществляется пропускной режим.

6.6.5. Технические меры защиты должны быть основаны на использовании различных программ и электронных устройств, выполняющих функцию защиты, и направлены на обеспечение правильности функционирования системы защиты и целостности хранимой и обрабатываемой информации. Среди них выделяют следующие меры:

- непрерывное поддержание необходимого уровня защищенности информационной системы персональных данных Общества,
- применение средств защиты информационной системы персональных данных и непрерывная административная поддержка их использования,
- использование средств антивирусной защиты, резервного копирования и восстановления программных средств информационной системы персональных данных,
- использование средств аутентификации и идентификации пользователей (персональные компьютеры, на которых содержатся персональные данные, должны быть защищены паролями доступа),
- использования средств разграничения прав доступа к персональным данным.

Конкретный перечень технических средств защиты должен быть определён отдельно для каждой информационной системы персональных данных.

6.7. Между Обществом и лицом, занимающимся обработкой персональных данных заключается соглашение, в котором должен быть указан порядок работы с персональными данными.

7. Передача персональных данных субъектов

7.1.Передача персональных данных осуществляется в соответствии с положениями Российского законодательства.

7.2. Общество обеспечивает ведение книги учета выданных персональных данных Субъектов персональных данных, в котором регистрируются запросы, фиксируются сведения о лице, направившем зарос, дата передачи персональных данных, а так же отмечается, какая именно информация была передана.

7.3. В случае осуществления Обществом трансграничной передачи персональных данных Субъекта на территорию иностранного государства трансграничная передача осуществляется с соблюдением требований действующего законодательства Российской Федерации и международно-правовых норм.

8. Ответственность и полномочия

8.1. Устанавливается ответственность:

- за управление настоящим документом – помощник генерального директора по кадрам и общим вопросам,
- за сохранность носителя и конфиденциальность персональных данных – каждый сотрудник Общества, занимающийся обработкой персональных данных,
- за осуществление контроля над соблюдением требований Политики - помощник генерального директора по кадрам и общим вопросам,
- за актуализацию локальных документов, содержащих списков должностей, уполномоченных на обработку персональных данных и (или) имеющих доступ к персональным данным работников – начальник отдела кадров,
- за обеспечение защиты, безопасности и отсутствия несанкционированного доступа к данным, находящимся в информационных системах Общества – начальник отдела автоматизированных систем управления.

8.2. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданских (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

8.3.Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника привлекается к дисциплинарной и материальной ответственности.

Разработано:

Помощник генерального директора
по кадрам и общим вопросам
_____Е.В. Насекина
«_09_»_10_____2019г.

Согласовано:

Директор по ЭиФ ОАО «СМЗ»
_____Г.И. Петухова
«_28_»_10_____2019 г.

Директор по правовым вопросам
_____О.В. Лесникова
«_09_»_10_____2019г.

Начальник АСУ
_____С.Г. Сурков
«_14_»_10_____2019г.

Начальник службы безопасности
_____Ю.В. Сибиряков
«_09_»_10_____2019г.

Начальник ОКа
_____Т.Е. Тревель
«_10_»_10_____2019г.