**СОГЛАШЕНИЕ**

**о взаимодействии в сфере информационной безопасности № ХХХХХ**

|  |  |
| --- | --- |
| г. Москва | « » 2022 года |

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем Сторона-1, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и
2. **Публичное акционерное общество «Новолипецкий металлургический комбинат» (ПАО «НЛМК»)**, юридическое лицо, созданное согласно законодательству Российской Федерации, место нахождения и реквизиты которого приведены в Разделе 17 «Адреса, реквизиты и подписи сторон», именуемое в дальнейшем Сторона-2, в лице Директора Дирекции по инфраструктуре и информационной безопасности Медвенского Леонида Игоревича, действующего на основании Доверенности № ДОВ-СО-1010-2000/2022 от 13.01.2022,

с другой стороны, именуемые в дальнейшем при совместном упоминании Стороны, заключили настоящее соглашение (далее – «Соглашение») о нижеследующем:

**ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

В настоящем Соглашении применены следующие термины с соответствующими определениями:

**«Автоматизированная система управления технологическим процессом» (АСУ ТП)** – комплекс программных и программно‑аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления таким оборудованием и процессами.

**«Акт о выявленном нарушении/Акт»** – документ, составляемый Стороной-2 в случае обнаружения неисполнения или ненадлежащего исполнения условий настоящего Соглашения Стороной-1 и/или Привлеченными лицами, и содержащий подробную информацию о таком несоответствии, соответствующий порядок оформления которого определен в разделе 7 настоящего Соглашения.

**«Государственный орган»** – все органы государственной власти и/или муниципальные органы, которым подведомственны, поднадзорны отношения в сфере защиты информации, обработки и защиты персональных данных, безопасности критической информационной инфраструктуры Российской Федерации, а также любые иные органы государственной власти и/или муниципальные органы, которые могут участвовать в процессе исполнения Договоров в части выдачи согласований, разрешений, заключений, проведения сертификаций, испытаний.

**«Договор»** – договор и/или соглашение между Стороной-1 и Стороной-2, предусматривающее выполнение работ /оказание услуг с использованием информационных систем, автоматизированных систем управления технологическим процессом, принадлежащих Стороне-2, на объектах критической информационной инфраструктуры Стороны-2, выполнение работ по техническому и сервисному обслуживанию оборудования и объектов ИТ-инфраструктуры Стороны-2, оказание услуг по внедрению, сопровождению, поддержке, модернизации информационных систем, автоматизированных систем управления технологическим процессом, принадлежащих Стороне-2, и/или других видов работ (услуг), предусматривающих получение доступа (включая удаленный) к информационным системам Стороны-2.

**«Законодательство»** – означает применяемые положения Конституции, нормативно-правовых актов, законов, кодексов, правил, положений, постановлений и распоряжений государственных органов законодательной и исполнительной власти.

**«Информационная система» (ИС)** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**«Инцидент информационной безопасности»** – событие или комбинация событий, указывающая на свершившееся, предпринимаемое нарушение информационной безопасности.

**«Привлеченные лица»** – лица, привлеченные Стороной-1 для выполнения работ по Договорам (включая, без ограничений, субподрядчиков, консультантов, аудиторов, поставщиков), работники таких лиц, привлеченных Стороной-1, а также иные лица, заявленные Стороной-1 в качестве работников/представителей Стороны-1 или работников/представителей лиц, привлеченных Стороной-1.

**«Систематическое нарушение»** – совокупность нарушений, совершенных Стороной-1 и/или Привлеченными лицами в течение календарного года либо на дату завершения работ по Договору и указанных в Разделах 1-3 Приложения № 1.

**«Существенное нарушение»** – однократное совершение Стороной-1 и/или Привлеченными лицами нарушений, указанных в Разделе 4 Приложения № 1, которое повлекло за собой нарушение нормальной деятельности (технической, информационной или корпоративной) Стороны-2, а также причинение последней ущерба и/или убытков.

Определения, употребляемые выше в единственном числе, могут употребляться также и во множественном числе, где это требуется по смыслу настоящего Соглашения.

Слова, термины и аббревиатуры, используемые в настоящем Соглашении со ссылкой на законодательство или без такой ссылки, но имеющие четкое определение в законодательстве, следует толковать в соответствии с законодательством.

Слова, термины и аббревиатуры, используемые в настоящем Соглашении без определения, но имеющие общепризнанное техническое или коммерческое значение в Российской Федерации, используются в настоящем Соглашении в наиболее всеобъемлющем и широком толковании указанного общепризнанного значения в Российской Федерации.

1. **ПРЕДМЕТ СОГЛАШЕНИЯ**
   1. Предметом настоящего Соглашения является организация взаимодействия Сторон в целях соблюдения требований нормативных документов в области защиты информации, безопасности критической информационной инфраструктуры Российской Федерации, при выполнении работ/оказании услуг для производственных нужд Стороны-2 в рамках исполнения договорных обязательств.
   2. Стороной-1 по настоящему Соглашению является юридическое или физическое лицо, выполняющее работы/оказывающее услуги для производственных нужд Стороны-2 по Договору.
   3. Сторона-1 признает ответственность перед Стороной-2 за неисполнение и/или ненадлежащее исполнение обязательств по настоящему Соглашению и Договорам, действующим на момент подписания настоящего Соглашения и/или заключенным Сторонами в пределах срока действия настоящего Соглашения.
2. **ПРИНЦИПЫ СОГЛАШЕНИЯ**

Стороны признают, что

* соблюдение требований законодательства в области защиты информации, безопасности критической информационной инфраструктуры Российской Федерации;
* повышение уровня компетенций работников в области защиты информации, безопасности критической информационной инфраструктуры Российской Федерации;

являются существенными условиями настоящего Соглашения и соблюдение Сторонами вышеуказанных положений является важнейшим аспектом деятельности Сторон.

1. **СРЕДСТВА БЕЗОПАСНОСТИ** 
   1. При выполнении работ Сторона-1 обязуется обеспечить соблюдение применимых к данному Соглашению требований действующего законодательства в области защиты информации, безопасности критической информационной инфраструктуры Российской Федерации, а также нормативных документов Стороны-2 в области информационной безопасности, приведенных в Приложении № 3 к настоящему Соглашению.
   2. При появлении в процессе выполнения работ необходимости в организации и проведении дополнительных разумно обоснованных мероприятий, требующихся по мнению Стороны-2 для защиты её информации, включая, но не ограничиваясь, введение в действие локальных нормативных документов Стороны-2 в сфере информационной безопасности, Сторона-2 обязана уведомить об этом Сторону-1, предоставить возможность ознакомления с актуальными локальными нормативными документами в сфере информационной безопасности и потребовать их выполнение в безусловном порядке.
2. **ОБЯЗАННОСТИ СТОРОНЫ-2**

Обеспечить выполнение мероприятий по защите информации, безопасности критической информационной инфраструктуры Российской Федерации, в том числе своевременное предоставление доступа Стороне-1 к ИС/АСУ ТП Стороны-2 в соответствии с порядком, установленным Стороной-2.

1. **ПРАВА СТОРОНЫ-2**
   1. Контролировать действия Стороны-1 в ИС/АСУ ТП Стороны-2 в рамках действующих Договоров.
   2. В случае выявления фактов совершения Стороной-1 Систематических и/или Существенных нарушений требований нормативных документов Стороны-2 в области защиты информации, безопасности критической информационной инфраструктуры Российской Федерации отстранять нарушителя от выполнения работ с ИС/АСУ ТП Стороны-2 с возможным последующим запретом на выполнение любых работ с ИС/АСУ ТП Стороны-2.
2. **ОБЯЗАННОСТИ СТОРОНЫ-1** 
   1. До начала выполнения работ /оказания услуг по Договору обеспечить информирование сотрудников Стороны-1/Привлеченных лиц об обязательствах, изложенных в настоящем Соглашении, а также о недопущении нарушений, указанных в Приложении 1 к настоящему Соглашению.
   2. Организовать выполнение работ/оказание услуг в полном соответствии с действующими нормативными документами Российской Федерации по защите информации при непосредственной работе в ИС/АСУ ТП Стороны-2, а также на объектах критической информационной инфраструктуры Стороны-2.
   3. Осуществлять контроль соблюдения работниками Стороны-1 применимых к данному Соглашению требований норм и правил по защите информации, безопасности критической информационной инфраструктуры Российской Федерации и мер для предотвращения нарушений, указанных в Приложении 1 к настоящему Соглашению.
   4. Предоставлять представителям Стороны-2 право проверки выполнения требований по защите информации при работе в ИС/АСУ ТП Стороны-2, безопасности критической информационной инфраструктуры Российской Федерации, а также не позднее 5 (пяти) рабочих дней с момента получения письменного уведомления Стороны-2 (либо в иной срок, установленный Стороной-2) направлять документы, подтверждающие соблюдение данных требований. Перечень указанных документов и способ передачи согласуются Сторонами дополнительно.
   5. Устранять нарушения и несоответствия, выявленные и доказанные представителями Стороны-2, в сроки, указанные в Акте.
   6. Сообщать Стороне-2 обо всех Инцидентах информационной безопасности, относящихся к Стороне-2, незамедлительно, но не позднее 1 часа с момента обнаружения Инцидента информационной безопасности.
   7. В случае привлечения Стороной-1 с письменного согласия Стороны-2 третьих лиц, в порядке, установленном Договорами, Сторона-1 обязана включить в заключаемые договоры с указанными лицами условия о соблюдении требований и применении ответственности в области защиты информации, безопасности критической информационной инфраструктуры Российской Федерации, предусмотренные настоящим Соглашением. Сторона-1 несет безусловную ответственность за осуществление контроля, ознакомление и исполнение требований и условий в области защиты информации, безопасности критической информационной инфраструктуры Российской Федерации, установленных настоящим Соглашением привлеченными третьими лицами. В случае выявления нарушений третьими лицами, привлеченными Стороной-1, требований в области защиты информации, безопасности критической информационной инфраструктуры Российской Федерации Сторона-1 несет ответственность за данные нарушения как за свои собственные.
3. **ПОРЯДОК УСТАНОВЛЕНИЯ ФАКТА НАРУШЕНИЯ. ДЕЙСТВИЯ СТОРОН ПО ОБМЕНУ ИНФОРМАЦИЕЙ И ДОКУМЕНТАМИ ПРИ УСТАНОВЛЕНИИ ФАКТА НАРУШЕНИЯ**
   1. Факт нарушения подтверждается Актом о выявленном нарушении, который составляется уполномоченным представителем/работником Стороны-2.

О выявленном нарушении Сторона - 2 обязана незамедлительно уведомить Сторону-1 в письменном виде.

В случае обнаружения неисполнения или ненадлежащего исполнения условий настоящего Соглашения Стороной-1 или Привлеченными лицами, представитель/работник Стороны-2 имеет право оформить Акт, который составляется не позднее 5 (пяти) рабочих дней с момента выявления нарушения.

В Акте указывается:

1. наименование ИС/АСУ ТП, при работе с которыми было выявлено нарушение;
2. дата, время совершения нарушения;
3. описание нарушения с обязательным указанием пункта и наименования нормативного документа, требования которого были нарушены;
4. сведения о нарушителе (фамилия, имя, отчество физического лица (нарушителя), профессия (должность);
5. сведения о предприятии (организации), работником которого является нарушитель;
6. негативные последствия (при наличии), которые наступили и/или могут наступить для Стороны – 2 в результате нарушения условий настоящего Соглашения,
7. срок устранения нарушения.
   1. Представитель/работник Стороны-2, проводящий проверку, вправе осуществить фото- или видеосъемку факта нарушения и приложить их к Акту в качестве доказательств, подтверждающих факт выявленного нарушения.
   2. Акт подписывается лицом, проводящим проверку, нарушителем/уполномоченным представителем предприятия, работником которого является нарушитель, другими лицами, в случае их участия (присутствия) в проверке. При этом нарушитель/уполномоченный представитель предприятия, работником которого является нарушитель, вправе указать в Акте свои пояснения по факту выявленного нарушения. При отказе виновного лица и/или уполномоченного представителя Стороны-1, работником которого является нарушитель, от подписания Акта в нём делается соответствующая отметка. Факт отказа от подписания Акта удостоверяется подписями лиц, участвующих в расследовании обстоятельств выявленного нарушения.
   3. В случае согласия нарушителя (уполномоченного представителя предприятия, работником которого является нарушитель) с содержанием Акта, данный документ считается достаточным и безусловным подтверждением факта нарушения требований, указанных в настоящем Соглашении. Акт направляется Стороне-1 для сведения и принятия мер по исключению повторения нарушения. Сторона-1 обязана в течение 5 (пяти) рабочих дней с момента получения Акта направить Стороне-2 письменное сообщение о принятых мерах и проведенных мероприятиях по устранению нарушений.
   4. В случае немотивированного отказа нарушителя (уполномоченного представителя предприятия, работником которого является нарушитель) от подписания Акта, или в случае несогласия нарушителя (уполномоченного представителя предприятия, работником которого является нарушитель) с обстоятельствами, изложенными в Акте, Сторона-2 обязана направить односторонне подписанный Акт Стороне-1 для рассмотрения.

Сторона-1 обязана в течение 3 (трёх) рабочих дней с момента получения Акта направить Стороне-2 подписанный Акт или мотивированный отказ от его подписания. В случае мотивированного отказа, Стороны в 10-дневный срок проводят дополнительную проверку обстоятельств выявленного нарушения.

В случае ненаправления Стороной-1 подписанного Акта или мотивированного отказа от его подписания односторонне подписанный Акт Стороной-2 является достаточным доказательством наличия выявленных нарушений в рамках исполнения настоящего Соглашения.

Направление Акта и/или иных документов, связанных с рассмотрением Акта, осуществляется посредством электронной почты с использованием электронных адресов контактных лиц, указанных в Разделе 17 настоящего Соглашения и/или почтовой корреспонденцией.

* 1. Акт, составленный и рассмотренный с соблюдением вышеуказанных требований, признается Сторонами надлежащим доказательством факта нарушения обязательств.

1. **ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** 
   1. В случае совершения Стороной-1 и/или Привлеченными лицами нарушений, указанных в Приложении № 1, а также при причинении имущественного ущерба Стороне-2   
      Сторона-1 несёт ответственность в виде уплаты штрафа и возмещения убытков.
   2. Претензия с требованием об уплате штрафа/возмещении убытков (далее – Претензия) предъявляется Стороне-1 в случае выявления Систематических и/или однократных Существенных нарушений требований нормативных документов в области защиты информации, безопасности критической информационной инфраструктуры Российской Федерации при выполнении работ/оказании услуг на ИС/АСУ ТП Стороны-2.

Критерии определения Систематического нарушения в зависимости от количества нарушений приведены в Приложении № 2.

Претензии за Систематические нарушения выставляются в первом квартале года, следующего за годом, в течение которого совершены нарушения. В случае если срок выполнения работ (оказания услуг) Стороны-1 по Договору составляет менее 1 (одного) года, а также в случае, когда нарушения совершены в отчетном году, в котором работы должны быть сданы Стороне-2, претензии за Систематические нарушения выставляются в течение 3 (трех) месяцев после окончательной приемки работ (оказания услуг).

* 1. Претензия об уплате штрафа направляется Стороне-1 почтовой корреспонденцией и/или на адрес электронной почты Стороны-1, указанный в настоящем Соглашении. К претензии прилагаются Акты о нарушениях, составленные в порядке, установленном настоящим Соглашением.
  2. Сторона-1 в течение 10 (десяти) рабочих дней с момента получения Претензии обязана рассмотреть ее, по результатам рассмотрения оплатить или направить   
     Стороне-2 на адрес ее электронной почты письменный отзыв на Претензию. При оплате Претензии банковские расходы несет Сторона-1. В случае невозможности оплаты Претензии в рублях РФ, Стороны дополнительно согласовывают банковские реквизиты Стороны-2, валюту платежа и курс пересчета суммы штрафа в валюту платежа. Неоплата, оставление без рассмотрения и ответа Претензии Стороной-1 является основанием для уменьшения цены любого Договора на сумму Претензии и/или проведения Стороной-2 зачета претензионной суммы в одностороннем порядке, путем прекращения своего встречного обязательства по любому Договору, заключенному Стороной-2 со Стороной-1, по которому Сторона-2 имеет перед Стороной-1 встречные однородные обязательства. Если Сторона-1 не согласна с фактом вменяемого ей нарушения она вправе направить Стороне-2 отзыв на Претензию, который последняя обязана рассмотреть и дать мотивированный ответ.
  3. Сторонысогласились, что обмен электронными копиями документов в порядке п.п. 8.3, 8.4 настоящего Соглашения является достаточным и не требует обмена оригиналами документов. Любая Сторона вправе потребовать предоставления оригинала документа, направленного ей другой Стороной по электронной почте.
  4. Размеры штрафов за совершённые нарушения указаны в Приложении № 2.   
     В зависимости от объема выполняемых Стороной-1 работ/услуг, объема предоставленного Стороне-1 доступа в ИС/АСУ ТП Стороны-2, уровня воздействия работ/услуг Строны-1 на объекты критической информационной инфраструктуры Стороны-2, размер штрафа может быть изменен.

1. **РАССМОТРЕНИЕ СПОРОВ**
   1. Споры, возникшие между Сторонами при исполнении настоящего Соглашения, подлежат рассмотрению в суде по месту нахождения Стороны-2 в соответствии с законодательством Российской Федерации.
   2. До обращения с иском в суд Сторона, чьи интересы нарушены, обязана предъявить претензию другой Стороне, на которую последняя обязана ответить в 30-дневный срок с момента её получения. Претензия может быть отправлена посредством электронной почты на электронные адреса Сторон, указанные в Разделе 17 настоящего Соглашения.

Претензии, отправленные таким способом, имеют полную юридическую силу и считаются доставленными адресату с момента получения отправителем автоматического ответа почтового сервера адресата о доставке электронного письма (или с момента отправки электронного письма, если функция автоматического ответа на сервере получателя не настроена либо отключена).

Надлежащим подтверждением отправки и получения претензий электронной почтой является печатная версия текста электронного письма с приложенным экземпляром претензии, заверенные подписью и печатью отправителя. Досылка оригиналов претензионных материалов, отправленных посредством электронной почты, не является обязательным условием, но может быть осуществлена по адресам, указанным в Разделе 17 настоящего Соглашения.

Порядок предъявления и рассмотрения претензий, установленный настоящим разделом, не распространяется на порядок выставления и рассмотрения Претензий Стороны-2 к Стороне-1 за нарушение требований по защите информации, безопасности критической информационной инфраструктуры Российской Федерации, который регулируется разделом 8 настоящего Соглашения.

1. **ЗАВЕРЕНИЯ ОБ ОБСТОЯТЕЛЬСТВАХ И ВОЗМЕЩЕНИЕ ПОТЕРЬ**
   1. В соответствии со ст. 431.2 ГК РФ Сторона-1 настоящим предоставляет Стороне-2 заверения о следующих обстоятельствах, имеющих значение для заключения, исполнения и/или прекращения настоящего Соглашения:
      1. Лицо, заключающее (подписывающее) Соглашение, действует в пределах полномочий, определенных действующим к дате заключения Соглашения Уставом/доверенностью.
      2. Сторона-1 получила все необходимые корпоративные одобрения Соглашения в порядке, предусмотренном действующим законодательством, в том числе, если Соглашение является для нее крупной сделкой или сделкой с заинтересованностью.
      3. Сторона-1 имеет соответствующие лицензии (разрешения) для выполнения Соглашения (если требуется лицензия) и нет никаких обстоятельств, которые могут повлиять на действительность лицензии (разрешения) в течение всего срока действия Соглашения.
      4. Сторона-1 обладает и будет обладать в течении срока действия Соглашения достаточными возможностями для своевременного и полного (надлежащего) исполнения своих обязательств по Соглашению.
      5. Сторона-1 не находится в процессе реорганизации или ликвидации.
      6. В отношении Стороны-1 не возбуждались и не осуществляются процедуры банкротства и отсутствуют какие-либо основания для возбуждения процедур банкротства в отношении Стороны-1.
      7. Сторона-1 не является участником (стороной) исполнительного, административного, гражданского, уголовного, налогового и т.д. производства (дела), которое бы повлияло на способность Стороны-1 исполнить свои обязательства по настоящему Соглашению.
      8. Сторона-1 оценила все свои риски, связанные с исполнением настоящего Соглашения (в т.ч. с уплатой штрафов, убытков, неустоек).
      9. Стороной-1 уплачиваются все налоги и сборы в соответствии с действующим законодательством, а также ведётся и своевременно подаётся в налоговые и иные Государственные органы налоговая, статистическая и иная государственная отчетность.
      10. Стороной-1 осуществляется предпринимательская (хозяйственная) деятельность в соответствии с требованиями действующего законодательства и отсутствуют факты, которые прямо или косвенно могут повлиять на исполнение договорных (налоговых) обязательств.
      11. Сторона-1 имеет руководителя и достоверный юридический адрес согласно действующему Уставу и учредительным документам.
      12. Сторона-1 имеет свидетельство о государственной регистрации, свидетельство о постановке на налоговый учёт.
      13. У Стороны-1 отсутствуют факты предоставления документов в налоговый орган с заведомо недостоверными сведениями.
      14. Сторона-1 не ведет деятельность, не направленную на получение прибыли. Исключение составляют юридические лица, основная деятельность которых согласно учредительным документам не направлена на извлечение прибыли.
      15. У Стороны-1 отсутствуют несоответствия показателей отчетности по сравнению со сведениями о движении денежных средств на расчетных счетах.
      16. Сторона-1 имеет в наличии основные средства и трудовые ресурсы для целей ведения производственно-хозяйственной деятельности.
      17. У Стороны-1 отсутствуют факты регистрации организации и представления отчетности через представителя по доверенности. Если названные действия осуществлялись / осуществляются представителем Стороны-1 по доверенности, то Сторона-1 заверяет, что такой представитель действительно уполномочен Стороной-1.
      18. У Стороны-1 отсутствуют факты неуплаты/неполной уплаты налогов и/или таможенных платежей по всей цепочке взаимозависимых лиц со Стороной-1. Для целей исполнения настоящего пункта взаимозависимыми лицами являются лица, способные оказывать влияние на условия и (или) результаты сделок, совершаемых Стороной-1 и /или экономические результаты деятельности указанных лиц.
      19. У Стороны-1 отсутствуют факты незаконного вывода денежных средств за границу.
      20. Сторона-1 соблюдает нормы, обеспечивающие права человека, установленные международно-правовыми актами и соглашениями, а также законодательством РФ, в том числе: право на свободу собраний и объединений, право на свободу и личную неприкосновенность, запрет использования принудительного и детского труда, запрет на дискриминацию по половому признаку, социальному статусу, на основе вероисповедания или расовой принадлежности, право на обеспечение безопасных условий труда, право на охрану труда и здоровья людей, право на получение гарантированного минимального размера оплаты труда, установленного законодательством, применимым к Стороне-1.
   2. Сторона-1 обязуется не позднее 3 (трех) рабочих дней предоставить Стороне-2 уведомление об изменении обстоятельств и данных, указанных в п. 10.1**.**
   3. Заверения Стороны-1 имеют для Стороны-2 существенное значение. Сторона-2 приняла решение о заключении Соглашения со Стороной-1 на условиях, указанных в настоящем Соглашении, с учётом заверений Стороны-1. Сторона-2 не заключала бы Соглашение или заключила бы его на иных условиях, если бы имела сведения о недостоверности вышеуказанных заверений Стороны-1.
   4. В соответствии со ст. 406.1 ГК РФ, Сторона-1 обязуется, в течение 5 (пяти) рабочих дней с даты соответствующего требования Стороны-2, возместить имущественные потери Стороны-2, возникшие в случае наступления любого из следующих обстоятельств:
      1. Предъявление Стороне-2 всех претензий, требований, судебных исков и т.п. со стороны Государственных органов, имеющих право выносить властные предписания, обязательные к исполнению, в связи с действиями Стороны-1 при исполнении настоящего Соглашения.
      2. Предъявление Стороне-2 претензий, требований и судебных исков со стороны третьих лиц, которые могут возникнуть в связи с исполнением Стороной-1 настоящего Соглашения, включая, без ограничений, нарушение требований нормативных документов в области защиты информации, безопасности критической информационной инфраструктуры Российской Федерации.
   5. Размер имущественных потерь, подлежащих возмещению Стороной-1 в соответствии с п. 10.4 равен совокупной сумме убытков, издержек и расходов, возникших у Стороны-2 в связи с наступлением указанных в п. 10.4 обстоятельств.
2. **КОНФИДЕНЦИАЛЬНОСТЬ**
   1. Стороны обязуются сохранять конфиденциальность условий Соглашения, любой иной информации, полученной в связи с исполнением Соглашения, а также всех прочих сведений, не являющихся общедоступными и касающихся Сторон и/или связанных с заключением и исполнением Соглашения (именуемых далее – «Конфиденциальная информация») и принять все возможные меры, чтобы предохранить полученную информацию от разглашения.

Сторона вправе раскрыть Конфиденциальную информацию, полученную от другой Стороны:

1. своим работникам, членам органов управления, а также своим аффилированным лицам, их работникам и членам органов управления;
2. своим аудиторам, а также аудиторам своих аффилированных лиц в той степени, в которой это необходимо для целей настоящего Соглашения или для целей подготовки бухгалтерской (финансовой) отчетности соответствующей Стороной или её аффилированными лицами;
3. в случаях, когда такое раскрытие необходимо или обязательно в соответствии с требованиями действующего законодательства, правил биржи и/или на основании обязательного для исполнения предписания органа государственной власти, контролирующего либо судебного органа;
4. в той степени, в которой это минимально необходимо для целей рассмотрения споров по настоящему Соглашению, а также споров с третьими лицами, связанных с исполнением Соглашения;
5. в части раскрытия Конфиденциальной информации Стороной-2 - для целей использования приобретенного по Договору Товара / результатов выполненных Работ / оказанных Услуг в рамках обычной хозяйственной деятельности Стороны-2;
6. в случае, когда Конфиденциальная информация становится общедоступной не по вине соответствующей Стороны.

Сторона-1 обязуется допускать к обработке Конфиденциальной информации Стороны-2 лиц, указанных в пункте 11.1 (а), только в связи с исполнением Соглашения или в рамках должностных обязанностей указанных лиц при условии принятия (наличия принятия) такими лицами обязательств о конфиденциальности в объеме, аналогичном положениям настоящего Соглашения.

11.2 Стороны договорились в рамках выполнения обязательств по настоящему Соглашению руководствоваться условиями и требованиями заключенного Сторонами Соглашения о конфиденциальности, если такое соглашение было заключено.

1. **ФОРС-МАЖОР**
   1. Стороны не несут ответственности за неисполнение (ненадлежащее исполнение) обязательств, предусмотренных настоящим Соглашением, если данное неисполнение (ненадлежащее исполнение) произошло вследствие стихийных явлений природы и запретительных мер государственных органов, наступивших после заключения настоящего Соглашения и препятствующих его полному или частичному исполнению.

Наступление таких обстоятельств при условии надлежащего уведомления в соответствии с условиями настоящего раздела продлевает срок исполнения обязательств по Соглашению соразмерно периоду действия форс-мажорного обстоятельства без возмещения убытков.

* 1. В случае наступления форс-мажорных обстоятельств, сторона, для которой такие обстоятельства возникли, обязана немедленно в письменной форме известить другую сторону о наступлении и прекращении действия этого обстоятельства, однако не позднее 5 (пяти) дней с момента их наступления/прекращения. В дальнейшем, подтверждением факта наступления и периода действия форс-мажорных обстоятельств является документ, выданный уполномоченным органом.

Сторона, затронутая этим обстоятельством, если своевременно не объявит о его наступлении, не может ссылаться на него, кроме случаев, когда само это обстоятельство препятствовало отправлению такого сообщения.

* 1. При возникновении форс-мажорных обстоятельств, стороны действуют из соображений минимизации возможных потерь и убытков.
  2. В случаях, когда обстоятельства непреодолимой силы продолжают действовать более 30 (тридцати) календарных дней, Стороны обязаны провести переговоры с целью выявления приемлемых для них альтернативных способов исполнения условий Соглашения.

1. **ПЕРЕДАЧА ПРАВ И ОБЯЗАННОСТЕЙ ПО СОГЛАШЕНИЮ**
   1. Стороны договорились о том, что передача прав и/или обязанностей Стороны-1 по настоящему Соглашению третьим лицам не допускается без предварительного письменного согласия Стороны-2. В случае, если Сторона-1 передала свои права (обязанности) по настоящему Соглашению третьим лицам без письменного согласия Стороны-2, Сторона-1 обязана уплатить штраф в размере 100 000 рублей, а также возместить убытки сверх суммы штрафа, возникшие в связи с такой передачей.
2. **АНТИКОРРУПЦИОННАЯ ПОЛИТИКА И ЗАВЕРЕНИЯ СТОРОН**
   1. Стороны настоящим подтверждают и гарантируют, что при заключении, а также при исполнении настоящего Договора, Стороны, их аффилированные лица, работники или посредники не совершали и не совершают действия, квалифицируемые применимым для целей Договора законодательством как дача/получение взятки, коммерческий подкуп, а также действия, нарушающие требования применимого антикоррупционного законодательства, а также законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем. В том числе, Стороны не выплачивают, не предлагают выплатить и не разрешают выплату каких-либо денежных средств или ценностей, прямо или косвенно, любым лицам, для оказания влияния на действия или решения этих лиц с целью получить какие-либо неправомерные преимущества или для достижения иных неправомерных целей.
   2. В случае получения Стороной информации о возможном (в том числе потенциальном) нарушении каких-либо положений настоящей статьи, соответствующая Сторона обязуется уведомить другую Сторону в письменной форме с указанием соответствующих фактов/приложением материалов, ставших основанием для такого уведомления (далее – «**Уведомление**»).

Каналы для направления Уведомления в адрес Сторон:

Сторона 1: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Сторона 2: [compliance@nlmk.com](mailto:compliance@nlmk.com)

В течение 10 (десяти) рабочих дней с даты получения Уведомления соответствующая Сторона обязана рассмотреть полученное Уведомление и сообщить другой Стороне об итогах его рассмотрения.

* 1. Стороны гарантируют осуществление надлежащего разбирательства по фактам нарушения положений настоящей статьи с соблюдением принципов конфиденциальности и применение эффективных мер по предотвращению возможных конфликтных ситуаций. Стороны подтверждают, что предпримут необходимые меры для защиты сотрудников, добросовестно сообщивших о нарушении настоящей статьи, от любых негативных последствий, связанных с таким сообщением.

1. **СРОК ДЕЙСТВИЯ, ИЗМЕНЕНИЕ, ДОПОЛНЕНИЕ И ПРЕКРАЩЕНИЕ СОГЛАШЕНИЯ**
   1. Соглашение (изменения, дополнения к нему) вступает в силу с момента подписания его (их) уполномоченными лицами Сторон, регистрации в Дирекции по правовым вопросам Стороны-2 и действует до полного исполнения обязательств. При этом подписи уполномоченных лиц Сторон должны быть скреплены печатью.
   2. С момента вступления в силу настоящего Соглашения иные заключенные между Сторонами соглашения в сфере информационной безопасности признаются расторгнутыми, при этом обязательства, возникшие до момента их расторжения, подлежат исполнению в полном объеме.
   3. Настоящее Соглашение, а также все изменения, дополнения и иная переписка к нему действительны, если подписаны уполномоченными лицами Сторон, имеющими право на совершение подобных действий согласно действующим Учредительным документам, либо другими лицами Сторон, имеющими доверенности на совершение подобных действий, оформленными в соответствии с действующим законодательством.

Каждая Сторона при подписании настоящего Соглашения, а также всех изменений, дополнений и иной переписки к нему вправе ознакомиться с оригиналами вышеуказанных документов или потребовать предоставления их копий, заверенных уполномоченными лицами соответствующей из Сторон.

* 1. Сторона-2 вправе в одностороннем порядке расторгнуть настоящее Соглашение без обращения в суд, предварительно письменно предупредив Сторону-1 за 20 (двадцать) дней до предполагаемой даты расторжения.
  2. Сторона-2 вправе расторгнуть действующие Договоры со Стороной-1 (помимо оснований, указанных в самих Договорах) в одностороннем внесудебном порядке и потребовать возмещения убытков, вызванных их расторжением в следующих случаях:

- Систематического (2 (двух) и более раз в течение календарного года)) совершения Существенных нарушений работниками Стороны-1 и/ или Привлеченных лиц;

- при появлении подтвержденных свидетельств Систематического нарушения Стороной-1 и/или Привлеченными лицами обязательств, изложенных в настоящем Соглашении, и игнорировании требований в области защиты информации, безопасности критической информационной инфраструктуры Российской Федерации Стороны-2.

* 1. При переписке обязательна ссылка на регистрационный номер Соглашения от Дирекции по правовым вопросам Стороны-2.

1. **ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ**
2. Перечень нарушений требований нормативных документов
3. Штрафы
4. Перечень нормативных документов в области информационной безопасности
5. **АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН**

|  |  |  |
| --- | --- | --- |
|  | **СТОРОНА-1** | **СТОРОНА-2** |
| Полное наименование предприятия |  | Публичное акционерное общество «Новолипецкий металлургический комбинат» |
| Краткое наименование предприятия |  | ПАО «НЛМК» |
| Юридический адрес |  | 398040, г. Липецк, пл. Металлургов, д. 2 |
| Почтовый адрес |  | 398040, г. Липецк, пл. Металлургов, д. 2 |
| Контактный телефон |  | +7 (4742) 442-222 |
| Электронная почта (e-mail) |  | [info@nlmk.com](mailto:info@nlmk.com) |
| ИНН |  | 4823006703 |
| КПП |  | 997550001 |
| ОГРН |  | 1024800823123 |
| Номер расчетного счета |  | 40702810500000114727 |
| Номер корсчета |  | 30101810000000000256 |
| Наименование банка |  | ПАО РОСБАНК |
| БИК |  | 044525256 |
| Адрес банка |  | 107078, г. Москва, ул Маши Порываевой, 34 |

|  |  |
| --- | --- |
| **Сторона-1:**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **М.П.** | **Сторона-2:**  **Директор Дирекции по инфраструктуре и информационной безопасности**  **ПАО «НЛМК»**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Л.И. Медвенский /**  **М.П.** |

**ПРИЛОЖЕНИЕ № 1**

**к Соглашению о взаимодействии в сфере информационной безопасности**

**от « » 2022 года № ХХХХХ**

**Перечень нарушений требований нормативных документов Стороны-2**

|  |  |
| --- | --- |
| **№**  **п/п** | **Наименование нарушения** |
| **Раздел 1. Нарушения требований нормативных документов при работе с информационными системами, автоматизированными системами управления технологическим процессом, принадлежащими Стороне-2, техническими средствами (персональный компьютер / мобильные устройства (ноутбуки, нетбуки, планшеты и мобильные телефоны) / сервисы сетевой печати и копировально-множительной техники), находящимися в собственности Стороны-2** | |
| **1.1** | Использование технических средств Стороны-2 для развлечений и других действий, не связанных с выполнением работ по Договору |
| **1.2** | Изменение настроек / отключение / удаление установленных средств защиты информации и мониторинга и контроля информационных ресурсов |
| **1.3** | Самостоятельный ремонт / изменение конфигурации технических средств / вскрытие системных блоков и иных компонентов технических средств, если такие действия не связаны с выполнением работ по Договору |
| **1.4** | Самостоятельная установка / внесение изменений в настройки операционной системы и прикладного программного обеспечения, если такие действия не связаны с выполнением работ по Договору |
| **1.5** | Использование систем виртуализации на рабочей станции |
| **1.6** | Работа в корпоративной сети Стороны-2 под чужой учетной записью |
| **1.7** | Работа в корпоративной сети Стороны-2 под учетной записью, имеющей права администратора; добавление учетных записей в привилегированные доменные группы и привилегированные локальные группы пользователей без согласования Управления информационной безопасности Стороны-2, если такие действия не связаны с выполнением работ по Договору |
| **1.8** | Организация ресурсов общего доступа и сетевых сервисов (открытие доступа к общим папкам, дискам, настройка служб удаленного доступа, беспроводных точек доступа), если такие действия не связаны с выполнением работ по Договору |
| **1.9** | Сканирование сетевых узлов по конечным устройствам или портам, если такие действия не связаны с выполнением работ по Договору |
| **1.10** | Подключение к сетям Стороны-2 с личных устройств, за исключением подключения с использованием личных мобильных устройств к системе корпоративной электронной почты и Skype for Business, удаленной работы с ресурсами Стороны-2, организованной посредством Cisco VPN или RDP-клиента |
| **1.11** | Предоставление доступа к техническому средству Стороны-2 посторонним лицам или другим работникам Стороны-1, не имеющим доступ к защищаемой информации и информационным системам, автоматизированным системам управления технологическим процессом Стороны-2 (за исключением лиц, обслуживающих технические средства Стороны-2), в том числе при отсутствии блокировки технического средства при покидании рабочего места |
| **1.12** | Осуществление попыток обхода существующих ограничений уровня доступа |
| **1.13** | Хранение и использование на технических средствах Стороны-2 программного обеспечения и файлов, не относящихся к производственной деятельности Стороны-2, объектов интеллектуальной собственности в нарушение прав их законных правообладателей |
| **1.14** | Сокрытие от Стороны-2 фактов инцидентов ИБ, относящихся к Стороне-2 |
| **Раздел 2. Нарушения требований нормативных документов по безопасности критической информационной инфраструктуры (КИИ) Российской Федерации** | |
| **2.1** | Внесение изменений в конфигурацию АСУ ТП и ее средства (механизмы) защиты, если такие действия не связаны с выполнением работ по Договору |
| **2.2** | Организация удаленного доступа к АСУ ТП в обход установленных средств защиты информации |
| **2.3** | Подключение и/или изменение настроек подключения к сети электрической связи оконечного оборудования объекта КИИ, если такие действия не связаны с выполнением работ по Договору |
| **2.4** | Попытки обхода существующих ограничений уровня доступа |
| **2.5** | Предоставление доступа к техническим средствам объекта КИИ посторонним лицам или другим работникам Стороны-1, не имеющим доступ к объекту КИИ Стороны-2 |
| **2.6.** | Изменение настроек / отключение / удаление установленных средств защиты информации и мониторинга и контроля информационных ресурсов на объектах КИИ Стороны-2 |
| **2.7.** | Сокрытие от Стороны-2 фактов инцидентов ИБ, связанных с функционированием объектов КИИ |
| **Раздел 3. Иные нарушения требований нормативных документов по информационной безопасности** | |
| **3.1** | Использование паролей, не отвечающих заданным требованиям сложности (длина - не менее 9 символов, состав - буквы латинского алфавита в верхнем и нижнем регистрах, цифры и, при наличии технической возможности, специальные символы ~ ! @ # $ % ^ & \* - \ | /?);), и включение в состав пароля легко вычисляемые сочетания и последовательности символов и знаков (111, qwerty, abcd, USER и т.п.) и другие угадываемые на основании знания информации о работнике (фамилия, дата рождения, номер авто, кличка питомца и т.п.) |
| **3.2** | Хранение аутентификационной информации (паролей) на бумажных и иных носителях в открытом виде на рабочем месте / в скриптах |
| **3.3** | Передача аутентификационной информации (паролей) третьим лицам или другим работникам Стороны-1 |
| **3.4** | Использование доступа в сеть Интернет из корпоративной сети Стороны-2 или с технических средств Стороны-2 для развлечений и других действий, не связанных с выполнением работ по Договору |
| **3.5** | Осуществление попыток обхода настроек прокси-серверов и фаерволов, ограничений доступа к ресурсам сети Интернет |
| **3.6** | Использование любых виртуальных и анонимных сетей (TOR, I2P и т.д.) из корпоративной сети Стороны-2 или с технических средств Стороны-2 |
| **3.7** | Распространение в корпоративной сети Стороны-2 (в том числе пересылка) фишинговых писем электронной почты, осуществление массовых рассылок |
| **3.8** | Сокрытие выявленных фактов нарушений информационной безопасности Стороной-1 |
| **Раздел 4. Существенные нарушения** | |
| **4.1** | Существенными считаются нарушения, приведенные в разделах 1-4 настоящего Приложения, последствия которых повлекли за собой:   * нарушение функционирования 1 (одного) и более технических средств Стороны-2 (за исключением технических средств, входящих в состав объекта КИИ) / сегмента корпоративной сети Стороны-2; * нарушение порядка обработки конфиденциальной информации Стороны-2 вследствие которого Стороне-2 причинен ущерб и/или убытки; * компрометацию учетной записи корпоративной сети Стороны-2 вследствие которой Стороне-2 причинен ущерб и/или убытки; * нарушение функционирования 1 (одного) и более технических средств, входящих в состав объекта КИИ; * нарушение функционирования бизнес-процессов и технологических (производственных) процессов Стороны-2; * инциденты ИБ, ставшие причинами развития кибератак на корпоративную сеть и ресурсы Стороны-2. |

|  |  |
| --- | --- |
| **Сторона-1:**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **М.П.** | **Сторона-2:**  **Директор Дирекции по инфраструктуре и информационной безопасности**  **ПАО «НЛМК»**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Л.И. Медвенский /**  **М.П.** |

**ПРИЛОЖЕНИЕ № 2**

**к Соглашению о взаимодействии в сфере информационной безопасности**

**от « » 2022 года № ХХХХХ**

**Штрафы**

|  |  |  |  |
| --- | --- | --- | --- |
| **Систематическое нарушение**  **(Приложение 1, разделы 1-4), руб.** | | | **Существенное нарушение (Приложение 1, раздел 4), руб.** |
| **При совершении 3 (трёх) нарушений за год** | **При совершении**  **5 (пяти) нарушений за год** | **При совершении**  **10 (десяти) нарушений за год, и за каждые последующие 10 (десять) нарушений** | **Каждое нарушение** |
| 300 000 | 500 000 | 800 000 | 1 000 000 |

|  |  |
| --- | --- |
| **Сторона-1:**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **М.П.** | **Сторона-2:**  **Директор Дирекции по инфраструктуре и информационной безопасности**  **ПАО «НЛМК»**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Л.И. Медвенский /**  **М.П.** |

**ПРИЛОЖЕНИЕ № 3**

**к Соглашению о взаимодействии в сфере информационной безопасности**

**от « » 2022 года № ХХХХХ**

**Перечень нормативных документов в области информационной безопасности**

1. Положение об обеспечении информационной безопасности П DIT-345-0024-2020.

|  |  |
| --- | --- |
| **Сторона-1:**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **М.П.** | **Сторона-2:**  **Директор Дирекции по инфраструктуре и информационной безопасности**  **ПАО «НЛМК»**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Л.И. Медвенский /**  **М.П.** |