Приложение 1 к документации о закупке

**Техническое задание**

**на оказание услуг по технической поддержке системы ITSM**

**для нужд АО «ЭнергосбыТ Плюс»**

1. **Общие сведения**
   1. **Цели сопровождения**

Основными целями оказания услуг по технической поддержке системы ITSM (далее Система) являются обеспечение её бесперебойного функционирования, обновление руководств пользователя и администратора, а также оперативное решение проблем, возникающих у пользователей при эксплуатации Системы.

* 1. **Заказчик**

АО «ЭнергосбыТ Плюс», далее по тексту (Заказчик).

* 1. **Требования к организационному объему услуг**

Услуги оказываются для нужд всех филиалов АО «ЭнергосбыТ Плюс»

* 1. **Требования к срокам** **оказания услуг**

Общий срок оказания Услуг: в течение 12 месяцев с даты подписания Договора, но не ранее 03.04.2026г.

* 1. **Требования к безопасности**
     1. Полные Требования к информационной безопасности (далее Требования ИБ) к исполнителю при осуществлении удаленного доступа к инфраструктуре заказчика указаны в приложении №2 к настоящему Техническому заданию.

* 1. **Взаимодействие сторон в рамках сопровождения**

Основным каналом обращения за технической поддержкой является сама система ITSM, установленная у Заказчика.

В случае нарушения работы Системы, невозможности регистрации и/или обработки обращения в Системе ITSM, Заказчик подает обращения на почтовый адрес или телефон Исполнителя, указанные в договоре.

Исполнитель:

* Обеспечивает обработку обращений, зарегистрированных в Системе на соответствующую конфигурационную единицу и рабочую группу Исполнителя;
* При заключении договора предоставляет дополнительные каналы обращения за технической поддержкой:

Номер телефона Исполнителя

Адрес электронной почты Исполнителя

* Оказывает Услуги, указанные в п.1.8 настоящего Технического задания в соответствии с правилами предоставления технической поддержки (Приложение 1 к настоящему Технического задания)
* Если инициатором услуг является Исполнитель, то Исполнитель информирует по электронной почте представителя Заказчика о необходимости выполнения определенных действий сотрудниками Исполнителя, регистрирует соответствующую заявку в Системе и отслеживает ход ее исполнения в указанные сроки.

На каждый вопрос Заказчика или на возникающую ошибку в Системе оформляется одно Обращение.

Отдельные услуги по технической поддержке могут требовать временной остановки работы Системы, при которой работа всех Пользователей невозможна. Плановой остановкой считается остановка системы в нерабочее время, о которой Заказчик и Исполнитель договариваются заранее и ставят в известность Пользователей.

Все плановые остановки Исполнитель согласует по электронной почте Заказчику не менее чем за 2 дня до оказания услуг.

Остановки, вызванные нарушениями в работе серверного оборудования и программного обеспечения, считаются неплановыми. В этих случаях Заказчик или Исполнитель извещает другую сторону по телефону или электронной почте о предполагаемом времени и длительности приостановки работы.

* 1. **Требования к функциональному объёму оказания услуг**

Исполнитель оказывает для Заказчика следующие услуги по сопровождению Системы:

* Информационно-техническое обслуживание Системы, включающее доступ к закрытому форуму поддержки Итилиум с возможностью скачивания новых версий Системы (ИТС «Итилиум» в наличии);
* Обновление Системы по мере выхода новых версий 1С Итилиум по запросу Заказчика;
* Консультирование пользователей и администраторов по вопросам эксплуатации системы;
* Консультирование пользователей и администраторов по решению проблем, возникающих при работе в Системе;
* Модификация правил;
* Проведение анализа и предоставление инструкций по исправлению ошибок, обусловленных действиями Пользователей;
* Устранение последствий ошибок Пользователей и сбоев Системы, в т.ч. восстановление нормального функционирования Системы и нормального состояния хранилища данных;
* Устранение ошибок программного обеспечения, приводящих к нарушению функционирования системы в штатном режиме согласно эксплуатационной документации;
* Контроль работоспособности компонент Системы, мониторинг объектов хранилища данных;
* Восстановление компонент Системы после сбоев – при необходимости;
* Мониторинг производительности Системы и предоставление рекомендаций по увеличению быстродействия;
* Расширение существующих и новых отчетов;
* Расширение существующей функциональности Системы и дополнительные услуги по Заявке Заказчика (Приложение №3 к настоящему Техническому заданию), их корректная интеграция в действующие механизмы, настройка их полного взаимодействия с типовыми решениями Системы для реализации бизнес-процессов Заказчика;
* Настройка обмена данными с различными программами Заказчика штатным функционалом Системы, в том числе, работающими на платформах, отличных от платформы Итилиум;
* Внесение корректировок и обновление пользовательских инструкций по работе с Системой;
* Прочие услуги, не указанные выше, связанные с функционированием Системы.

Объем оказываемых услуг – не менее 41 часа в сумме за отчетный период (месяц).

* 1. **Состав услуг, исключенных из объема сопровождения**

Перечень услуг, исключенных из объема сопровождения и сервисного обслуживания Системы. При необходимости данные услуги могут быть предоставлены по заявке Заказчика на отдельных условиях и по отдельным соглашениям.

* Оценка нового программного обеспечения или оборудования – Оценка или одобрение нового программного обеспечения или аппаратных средств для использования у Заказчика, включая системы, разработанные третьими лицами или самим Заказчиком;
* Приобретение нового программного обеспечения или оборудования – Приобретение нового программного обеспечения или аппаратных средств для использования у Заказчика или для применения у Исполнителя в интересах Заказчика. Всё программное обеспечение или аппаратные средства, необходимые Исполнителю для использования при поддержке Заказчика, являются ответственностью Заказчика и приобретаются за его счет;
* Лицензирование программного обеспечения – Исполнитель не поддерживает нелицензированное программное обеспечение и не предоставляет лицензии на программное обеспечение. Заказчик самостоятельно обеспечивает программное обеспечение необходимыми лицензиями и правами на использование;
* Обновление аппаратных средств – Заказчик обязан самостоятельно обновлять аппаратные средства серверной группы и поддерживать их в актуальном состоянии в соответствии с рекомендациями производителя;
* Помощь в использовании приложений – Советы или обучение настройкам и использованию приложений сторонних производителей, включая создание пользователей для этих приложений и т.п.;
* Помощь в поддержке среды прикладных программ – Советы по использованию, поддержке и обслуживанию среды прикладных программ, включая инструментальные средства разработки, прикладное программное обеспечение сервера и баз данных;
* Помощь при нестандартных решениях – Касается использования Заказчиком нестандартных аппаратных средств или программного обеспечения, не поддерживаемых производителями, что часто является причиной непредсказуемого и неожиданного поведения или ненадежной работы всей Системы;
* Адаптивное обслуживание – Любая деятельность, имеющая отношение к обновлению, модернизации или преобразованию программного обеспечения Системы и выходящая за рамки согласованных технических требований, вследствие установки у Заказчика новых версий среды, прикладного программного обеспечения, включая операционные системы, серверное и клиентское программное обеспечение, базы данных, сетевое оборудование и т.д.

1. **Объект сопровождения**
   1. **Функции Системы**

Информационная система управления ИТ-услугами предназначена для автоматизации процессов управления ИТ-услугами, в том числе управления ИТ-активами Заказчика, а также автоматизации следующих ИТ-процессов организации:

* Управление каталогом и уровнем услуг;
* Управление инцидентами и запросами на обслуживание;
* Управление услугами;
* Управление проблемами;
* Управление релизами;
* Управление изменениями;
* Управление конфигурациями;
* Управление активами
* Управление персоналом.
  1. **Задачи Системы:**
* Структурирование деятельности ИТ-подразделений, представив ее в виде Каталога услуг;
* Организация учета запросов, поступающих от пользователей, через единую точку контакта – службу «Service Desk»;
* Получение аналитической отчетность о поступающих запросах пользователей в разрезе услуг;
* Установка и контроль сроков обработки инцидентов и запросов, поступающих от пользователей;
* Предоставление клиентам интерфейса и инструмента подачи, отслеживания и оценки качества обработки их запросов;
* Поднятие удовлетворенности внутренних и внешних клиентов предоставляемыми услугами;
* Корректная оценка возможности по оказанию услуг при заключении Соглашения об уровне услуг;
* Учет трудозатрат сотрудников ИТ-подразделений в разрезе услуг/клиентов/сотрудников;
* Оказание и учет регламентных услуг по обслуживанию ИТ-инфраструктуры;
* Планирование и контролирование изменений в инфраструктуре, информационных системах и предоставляемых ИТ-услугах.
  1. **Архитектура Системы**

Система ITSM базируется на кластере серверов «1С: Предприятие 8» в клиент-серверном варианте, реализованном на основе трехуровневой архитектуры «клиент-сервер». Такая архитектура разделяет всю работающую систему на основные части, определенным образом взаимодействующие между собой:

* Клиентское приложение;
* Веб-сервер;
* Кластер серверов «1С: Предприятие»;
* Кластер серверов баз данных.
* Веб-портал Итилиум

Сервером лицензий 1С и Итилиума выступает один из серверов приложения 1С предприятия.

Клиентом системы ITSM выступают браузеры и клиенты 1С, установленные на ПК пользователей системы.

* 1. **Серверный состав системы ITSM**

Система располагается в виртуальной инфраструктуре центра обработки данных заказчика. Виртуальные машины, используемые для нужд системы, сконфигурированы и размещены на хостах кластеров, в ресурс-пулах и хранилищах, предоставленных заказчиком.

Все виртуальные машины, используемые для функционирования системы, располагаются в подсетях, обеспечивающих взаимодействие виртуальных машин и функциональных подсистем между собой и служебными сервисами заказчика.

| Наименование | Роль |
| --- | --- |
| msk-dmz-itsm | Публикация продуктивного сервера для внешнего веб-сервиса |
| msk-itsm-app02 | Сервер 1С Предприятия, сервер IIS, сервер лицензирования Итилиум и 1С. |
| msk-itsm-db01 | Сервер БД |
| msk-itsm-test17 | Тестовая среда. Тестовый сервер Приложений 1С для ИТСМ |
| msk-itsm-test16 | Тестовая среда. ИТСМ тест sql |
| msk-es04-app97 | Продуктивная среда bitrix - prod |
| msk-es04-app96 | Тестовая среда bitrix - test |
| msk-itsm-web01 | Форум |
| msk-es04-ts19  msk-es04-ts20 | Продуктивная среда терминалы коллекции ITSM |

Функциональные подсистемы ITSM взаимодействуют с почтовым сервисом заказчика в качестве почтового клиента по протоколам imap или pop для получения почты и smtp – для отправки. Взаимодействие с доменом осуществляется по протоколу LDAP для прозрачной авторизации в системе и синхронизации справочников бизнес-пользователей и исполнителей.

* 1. **Режим функционирования Системы**

Система функционирует в режиме многопользовательского доступа 24 часа в день, 7 дней в неделю.

1. **Контактные лица**

Перечень контактных лиц определяется в двустороннем порядке и оформляется после заключения договора на техническую поддержку. В случае замены контактных лиц сторона, осуществившая такую замену, должна уведомить противоположную сторону любым доступным способом в течение 2 рабочих дней.

**Приложения к Техническому заданию:**

Приложение №1 Правила предоставления технической поддержки;

Приложение №2 Требования по информационной безопасности;

Приложение №3 Форма заявки.

Приложение №1 к Техническому заданию

на оказание услуг по технической поддержке

системы ITSM на платформе Итилиум

**Правила предоставления технической поддержки**

1. **Термины**

**Инцидент** – несоответствие фактической работы Системы, предусмотренному в документации, появление окна с сообщением об ошибке, снижение быстродействия или зависание;

**Замечание** – замечание или предложение, поступившее от Пользователя по работе системы, связанное, в том числе, с расширением функциональности системы;

**Запрос на обслуживание** – изменение содержимого системных справочников, распределение ролей, настройка групп пользователей, правил обработки заявок и нарядов и иные задачи, связанные с настройкой содержимого Системы;

**Консультация** (запрос информации) – проведение пояснения Пользователю по работе в Системе, уточнение каких-либо непонятных моментов;

**Приоритет** – совокупная оценка степени влияния инцидента на бизнес-процессы Заказчика.

**Срок реакции** – это время, в течение которого Исполнитель обязуется приступить к работе над проблемой, обозначенной Заказчиком, способом, предусмотренным в этом соглашении.

**Обращение** – заявка, направленная в систему ITSM заказчика или направленная иным способом.

**Обходное решение** – метод, позволяющий избежать инцидента или проблемы с помощью временного решения или иным способом, устраняющим зависимость Потребителя от проблемных аспектов Системы.

**Эскалация** – процедура передачи запроса на более высокий уровень поддержки в случае, если его не удалось разрешить на текущем уровне.

1. **Порядок предоставления услуг**

Для получения услуг по Договору Заказчик направляет заявки в Систему ITSM. На каждый вопрос Пользователя или на возникающую ошибку в системе оформляется одно Обращение.

В случае невозможности регистрации и/или обработки Обращения в Системе ITSM, Заказчик подает Заявку в Сервис Деск Исполнителя по электронной почте или по телефону.

Обращение составляется на любое логически обособленное и ясно сформулированное требование Пользователя (специалиста Заказчика) на консультирование, предоставление услуг, поддержку и обслуживание, любое изменение или разрешение возникшей проблемы (ошибки) при работе с Системой.

Заявка может быть отправлена Пользователем в электронном виде на адрес Системы либо заведена самостоятельно, через интерфейс Системы. Порядок и правила оформления Заявок указываются в Правилах предоставления технической поддержки Системы.

Приоритет заявки указывается Заказчиком при подаче заявки

|  |  |
| --- | --- |
| Приоритет | Описание проблемы и действия Исполнителя по Заявке |
| Критичный | Заявка требует немедленной реакции и имеет критичное влияние на работоспособность приложения и выполнение бизнес-процессов. Приложение неработоспособно у пользователя, либо невозможно выполнение бизнес-процессов пользователем ни при каких условиях. Ситуация немедленно доводится до руководства Исполнителя. Проблема начинает решаться немед­ленно всеми возмож­ны­ми способами и ресурсами Исполнителя до ее полного разрешения. |
| Высокий | Имеет высокое влияние на работоспособность приложения и выполнение бизнес-процессов. Выполнение бизнес-процессов возможно каким-либо другим путем. Руководство Исполнителя ставится в известность о возникшей проблеме. |
| Средний | Не оказывает большого влияния на работоспособность приложения, минимально задействует функциональность основных бизнес-процессов. |
| Низкий | Имеет минимальное влияние на работоспособность приложения, не задействует работоспособность основных бизнес-процессов. |

1. **Время предоставления услуг при штатной работе Системы**
2. По рабочим дням (понедельник – пятница) с 07:00 до 16:00 часов (время московское), или по отдельному соглашению.
3. В праздничные, выходные дни по отдельному соглашению.
4. **Доступность, оперативность сервиса**

Исполнитель в рамках предоставления услуг по Договору будет прилагать все усилия для разрешения возникающих у Заказчика проблем в пределах, установленных в данном разделе норм с учетом времени предоставления услуг согласно п. 3.

Порядок обработки Заявок определяется их приоритетностью. Исполнитель рассматривает Заявки по мере их поступления. В случае если в момент поступления Заявки Исполнителем оказываются услуги над другой Заявкой с таким же приоритетом, то новая Заявка ставится в очередь. При необходимости Исполнитель сообщает Заказчику ориентировочный срок рассмотрения Заявки.

**4.1 Состав услуг, оказываемых Исполнителем в рамках взаимодействия через систему 1С Итилиум**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Поддержка бизнес-приложений (2-3 Линия)** | **1 Приоритет – Критический**  **(рабочий час)** | | **2 Приоритет – Высокий**  **(рабочий час)** | **3 Приоритет – Средний**  **(рабочий час)** | **4 Приоритет – Низкий (рабочий час)** |
| Консультирование | | - | 8 | 16 | 24 |
| Предоставление/изменение прав доступа | | - | 8 | 16 | 24 |
| Устранение некорректных действий пользователей | | 4 | 8 | 12 | 16 |
| Решение проблем/устранение сбоя (Решение Инцидента) | | 4 | 8 | 12 | 16 |
| Изменение данных/массовое изменение данных | | 4 | 16 | 32 | 80 |

1. **Управление нештатными ситуациями**

В случае если Исполнитель предвидит невозможность исполнения обязательств в соответствии с принятым уровнем сервиса или в полном объеме, Исполнитель должен немедленно уведомить ответственного представителя Заказчика и при необходимости разработать совместный план действий по разрешению нештатной ситуации.

Исполнитель должен вести реестр нештатных ситуаций, содержащий основные риски по всем типам услуг, и там, где возможно, механизмы их предотвращения. Исполнитель должен периодически пересматривать реестр и принимать разумные меры для снижения последствий нештатных ситуаций.

При возникновении нештатной ситуации исполнитель должен реагировать на заявку Заказчика в соответствии с Критичным приоритетом, независимо от Пункта 3 настоящего Приложения и отразить Фактические трудозатраты за Отчетный период в Акте оказанных Услуг.

1. **Регулярная отчётность**

Ежемесячно Исполнитель обязан предоставлять Заказчику следующую информацию о ходе оказания услуг:

| № | Документ | Порядок предоставления | Форма |
| --- | --- | --- | --- |
| 1 | Ежемесячный отчет о поступивших от Заказчика заявках по вопросам эксплуатации Системы, включающий следующую информацию:   * количество решенных инцидентов и объем часов, затраченных Исполнителем; * открытые заявки, сроки их решения; * план услуг на следующий месяц; * жалобы пользователей; * нарушение сроков реакции и сроков решения (фиксируется количество времени и причина просрочки по каждой заявке); * замечания и предложения сторон. | В электронном виде | Информационный отчет |
| 2 | Отчетные бухгалтерские документы о предоставленных услугах за отчетный период | В соответствии с договором | Акт оказанных услуг, счет и счет-фактура |

Приложение №2 к Техническому заданию

на оказание услуг по технической поддержке

системы ITSM на платформе Итилиум

от 13.10.2025

**ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

в части предоставления удаленного доступа третьим лицам, не являющихся работниками Общества (юридические лица, индивидуальные предприниматели, исполнители по договорам ГПХ, в том числе физические лица – плательщики НПД (самозанятые)), выполняющих работу и (или) оказывающих услуги по заказу Общества

1. **Термины и определения**
   1. Исполнитель, третье лицо – лицо, не являющееся работником Общества (юридические лица, индивидуальные предприниматели, исполнители по договорам ГПХ, в том числе физические лица – плательщики НПД (самозанятые)), выполняющее работу и (или) оказывающее услуги по заказу Общества.
   2. Заказчик, Общество - юридическое лицо, входящее в Группу компаний «Т Плюс».
2. **Нормативная база**
   1. Федеральный закон Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
   2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
   3. Федеральный закон Российской Федерации Ф от 27.07.2006 № 152-ФЗ «О персональных данных».
   4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
   5. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных.
   6. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
   7. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
   8. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности ЗОКИИ».
3. **Общие требования**
   1. Исполнитель при необходимости подключения собственного оборудования к ИТ-инфраструктуре Заказчика обязан предварительно в письменной форме согласовать такое подключение с Заказчиком и соблюсти требования по защите подключаемого оборудования не ниже класса защищенности 1Г в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
   2. Исполнитель для подключения собственного оборудования к сети Заказчика обязан:
      1. Предоставить аттестат соответствия требованиям защиты информации по классу не ниже «1Г» на подключаемое оборудование.
      2. Заключить соглашение о неразглашении информации (NDA) для оказания услуг в режиме удаленного доступа.
      3. Направить Заказчику заявку в установленной форме (п 4.4) с перечнем лиц, для которых необходимо предоставить удаленный доступ.
   3. Для оказания услуг Исполнителем в режиме удаленного доступа договор с Исполнителем должен содержать:

* оговорку о дистанционном характере оказания услуг;
* соглашение о полном соответствии настоящим Требованиям для подключения персонала Исполнителя к ИТ-инфраструктуре Общества.
  1. Все сведения о составе и характеристиках объектов Заказчика и их компонентах являются конфиденциальной информацией и распространению не подлежат в период действия договорных отношений и после прекращения договорных отношений в течение 10 лет (в случае, если иное не предусмотрено договором).
  2. Исполнитель обязуется:
* не проводить противозаконные действия (не ограничиваясь указанным: фальсификация, модификация, блокировка, уничтожение или искажение) по сбору, использованию и передаче третьей стороне информации, циркулирующей и хранящейся у Заказчика;
* не осуществлять несанкционированный доступ к информационным ресурсам Заказчика;
* не проводить незаконное копирование информации, циркулирующей или хранящейся у Заказчика;
* не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;
* не внедрять в объекты Заказчика программы-вирусы (загрузочные, файловые и др.);
* не устанавливать программные и аппаратные закладные устройства в технические средства Заказчика;
* не распространять конфиденциальную информацию о выполняемых работах и полученных результатах;
* использовать решения для удаленного доступа, определенные Заказчиком;
* использовать удаленный доступ только в целях исполнения договорных обязанностей между Исполнителем и Заказчиком.
  1. Авторизация работника Исполнителя должна осуществляться под персональными учетными записями, выданными Заказчиком. Использование чужих учетных записей, выданных другим работникам, не допускается.
  2. Работник Исполнителя должен принимать меры по защите предоставленных Заказчиком учетных данных и не допускать неавторизованного доступа других лиц к информационным ресурсам Заказчика.
  3. Исполнитель осуществляет дистанционное подключение к ресурсам Заказчика только с использованием статического IP адреса, согласованного с Заказчиком. Доступ с неизвестных Заказчику IP адресов может блокироваться техническими средствами Заказчика.
  4. Исполнитель обеспечивает выполнение условия, что все ресурсы, с которых осуществляется удаленное подключение, в том числе АРМ пользователя и другие технические средства и информационные сервисы, географически размещены на территории Российской Федерации.
  5. Запрещается подключение работников Исполнителя к ресурсам Заказчика с IP-адресов, расположенных за пределами РФ, (в том числе с использованием VPN-провайдеров, узлов TOR и подсетей хостинговых компаний (VPS/VDS), расположенных на территории РФ).
  6. При осуществлении удаленного подключения персонала Исполнителя к объектам информационной или технологической инфраструктуры Заказчика посредством не принадлежащего Заказчику компьютера или иного средства вычислительной техники (ноутбук, мобильное устройство, далее - Оборудование), если это предусмотрено Техническим заданием на работы, такое оборудование должно соответствовать следующим требованиям:
* на Оборудовании должно быть установлено лицензионное общесистемное программное обеспечение, находящееся на поддержке производителя, с установленными актуальными обновлениями, включая обновления безопасности;
* на Оборудовании должно быть установлено и функционировать сертифицированное средство антивирусной защиты, включённое в Единый реестр российских программ для ЭВМ и БД, с актуальными антивирусными базами (дата обновления не старше одного дня);
* отчет о полной проверке средством антивирусной защиты текущего состояния Оборудования (дата отчета не старше двух дней) не должен содержать событий выявления ВПО или иных событий безопасности.
  1. Удаленный доступ пользователей к информационным и/или технологическим ресурсам Заказчика, являющихся значимыми объектами критической информационной инфраструктуры (далее - ЗОКИИ), запрещен. В случае необходимости проведения работ на ЗОКИИ, подключение сторонних пользователей к таким объектам и их компонентам допускается только локально (очно) на территории площадок Заказчика.
  2. Исполнитель самостоятельно осуществляет выбор провайдера услуг Интернет, координацию установки оборудования и программного обеспечения, оплату соответствующих тарифов.
  3. Настройка и сопровождение оборудования, с которого осуществляется удалённый доступ к ресурсам Заказчика, а также установленного на оборудовании программного обеспечения, осуществляется Исполнителем.
  4. Запрещается использовать систему удаленного доступа для организации перманентного подключения сторонних сетей, в том числе локальных сетей Исполнителя.
  5. Заказчик с целью защиты своей ИТ-инфраструктуры, репутации и инвестиций, оставляет за собой право принимать любые меры контроля соблюдения Исполнителями настоящих требований по обеспечению необходимого уровня информационной безопасности. Отчет о соответствии указанным в пункте 3.11. требованиям может быть запрошен специалистами, ответственными за обеспечение информационной безопасности в Обществе, в любое время, а также при осуществлении оперативных мероприятий и расследовании инцидентов ИБ.
  6. Заказчик осуществляет контроль использования удаленного доступа к собственной инфраструктуре и может без предупреждения ограничить удаленный доступ в случае выявления нарушений настоящих требований.
  7. В случае компрометации, либо подозрения на компрометацию учетной записи или оборудования Исполнителя, Исполнитель обязан уведомить об этом инциденте Заказчика в кратчайший срок (не более 8 часов) с момента установления такого события.
  8. Исполнителем должна обеспечиваться регистрация событий безопасности, связанных с действиями пользователей при осуществлении удаленного доступа к ИТ-инфраструктуре Заказчика. Срок хранения таких событий должен составлять не менее 1 (одного) года.

Регистрации подлежат:

* для операционной системы Windows все события безопасности, содержащиеся по умолчанию в журнале «Безопасность»;
* для операционных систем семейства Linux все события безопасности, фиксируемые модулями аудита (например, auditd).
  1. В случае возникновения инцидента информационной безопасности, в том числе связанного с ИТ-инфраструктурой Исполнителя, Исполнитель по запросу Заказчика обязан предоставить журналы регистрации событий, указанных в пункте 3.19.
  2. Подключение к ИТ-инфраструктуре Заказчика осуществляется только в рабочие часы Заказчика. Удаленное подключение вне указанного временного интервала допускается при наличии обоснования необходимости такого подключения в соответствии с условиями договора.
  3. Доступ к ИТ-инфраструктуре Заказчика должен осуществляться со средств вычислительной техники, которые не используются в целях, не связанных с исполнением договорных или трудовых обязанностей Исполнителя, и соответствуют настоящим Требованиям.
  4. Для организации безопасного взаимодействия при удаленном доступе к ИТ-инфраструктуре Заказчика Исполнителем должен реализовываться базовый набор мер по информационной безопасности в соответствии с Приложением № 1 к настоящим Требованиям.

1. **Порядок оформления**
   1. Нарушение настоящих требований со стороны Исполнителя может влечь за собой в отношении Исполнителя административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации.
   2. Доступ работникам Исполнителя к объектам Заказчика предоставляется при условии выполнения настоящих требований, а также в соответствии с требованиями законодательства РФ.
   3. Доступ предоставляется, только определенному кругу лиц и устройств, которым разрешен удалённый доступ к программным и программно-аппаратным средствам объекта Заказчика.
   4. Форма предоставления сведений о перечне лиц и устройств Исполнителя, которым должен быть предоставлен удалённый доступ к программным и программно-аппаратным средствам:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | ФИО персонала Исполнителя | Статические IP-адреса, с которых будет осуществляться подключение (удаленного устройства). | MAC-адрес устройства, с которого будет осуществляться подключение (удаленного устройства). | Контактные данные (мобильный телефон и электронная почта). | Отметка (подпись и дата) об ознакомлении с мерами безопасности, об ознакомлении с ответственностью, о согласии на обработку персональных данных. | Адрес расположения устройства | Обоснование необходимости удаленного подключения к ИТ-инфраструктуре вне рабочие часы Заказчика\* (ссылка на пункт договора, временной интервал доступа) |
| *1.*  *…* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно  для  заполнения)* | *(Обязательно для заполнения)* | *(заполняется при необходимости)* |

*\*указывается пункт договора, являющийся обоснованием предоставления удаленного доступа вне рабочие часы Заказчика, и временной интервал такого доступа.*

* 1. Оригиналы заявок на предоставление доступа направляются Исполнителем в печатном и электронном виде Заказчику в рабочее время Заказчика. Заказчик рассматривает заявки в течение 5 рабочих дней со следующего рабочего дня после получения Заказчиком заявки на предоставление удаленного доступа. После рассмотрения заявки Заказчик в течение 3 рабочих дней направляет Исполнителю информацию о рассмотрении заявки.

1. **Порядок надзора за исполнением требований безопасности.** 
   1. Исполнитель обязан в полном объеме и определённые Заказчиком сроки выполнить все требования, направленные на выполнение Исполнителем мероприятий по обеспечению необходимого Заказчику уровня защиты информации. Под необходимыми требованиями понимаются требования, указанные в настоящем документе.
   2. Заказчик для контроля исполнения требований по защите информации имеет право:

* использовать имеющиеся у Заказчика средства контроля утечки конфиденциальной информации;
* использовать имеющиеся у Заказчика средства контроля действий пользователей;
* осуществлять контроль соблюдения Исполнителем требований по защите информации, в т.ч. требовать от Исполнителя предоставить используемую Исполнителем технику для проверки функционирования средств защиты информации в рамках действующих договорных отношений между Заказчиком и Исполнителем;
* при необходимости производить периодические проверки с предварительным согласованием Исполнителя на предмет возникновения нештатных ситуаций или инцидентов информационной безопасности путем имитации указанных событий (проведение тренировок);
* в случае необходимости запрашивать у Исполнителя политику информационной безопасности, результаты внутренних (внешних) аудитов информационной безопасности, результаты тестирования на проникновение ИТ-инфраструктуры Исполнителя, план реагирования на компьютерные инциденты, а также регламент действий работников Исполнителя в случае нештатных ситуаций.
  1. Заказчик имеет право в одностороннем порядке приостановить или прекратить предоставление удаленного доступа Исполнителю, а Исполнитель обязан выполнить связанные с этим решением мероприятия в сроки, обозначенные Заказчиком.
  2. Основания для непредоставления, приостановки или прекращения предоставления удаленного доступа:
* не предоставление Заказчику оригинала заявки, заполненной надлежащим образом;
* не исполнение (в т.ч. нарушение) со стороны Исполнителя требований Заказчика по защите информации, принадлежащей Заказчику, к которой Исполнитель получил доступ и которую он обрабатывал в рамках исполнения договорных отношений с Заказчиком;
* прекращение договорных отношений между сторонами;
* предписание федерального органа исполнительной власти Российской Федерации, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения, ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности информации Российской Федерации.

1. **Контактные лица для оперативного взаимодействия**
   1. При подозрении на возникновение инцидента информационной безопасности, связанного с удаленным доступом к ИТ-инфраструктуре Заказчика, взаимодействие между Заказчиком и Исполнителем должно осуществляться путем информирования ответственных лиц способами, приведенными в таблице № 1.

Таблица № 1 – Контактные данные для взаимодействия

|  |  |  |  |
| --- | --- | --- | --- |
| **Должность ответственного лица** | **Фамилия, имя, отчество** | **Телефон** | **E-mail** |
| **Заказчик** | | | |
| *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* |
| **Исполнитель** | | | |
| *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* |

* 1. Заказчик и Исполнитель в течение 5 рабочих дней со дня подписания договора осуществляют обмен контактными данными для взаимодействия в рамках реагирования на инциденты.
  2. Уведомление, содержащее контактные данные, направляется Исполнителем ответственному лицу со стороны Заказчика.
  3. В случае изменения контактных данных Заказчик и Исполнитель обязаны проинформировать друг друга о произошедших изменениях в течение 5 рабочих дней после их наступления.

Приложение № 1

к Требованиям по информационной безопасности в части предоставления удаленного доступа третьим лицам, не являющихся работниками Общества (юридические лица, индивидуальные предприниматели, исполнители по договорам ГПХ, в том числе физические лица – плательщики НПД (самозанятые), выполняющих работу и (или) оказывающее услуги по заказу Общества)

Перечень базовых мер

по информационной безопасности

В целях организации безопасного взаимодействия при наличии удаленного доступа к ИТ-инфраструктуре Группы «Т Плюс» организациям, оказывающим услуги в рамках заключенных договоров, необходимо обеспечить реализацию следующих базовых мер по информационной безопасности в собственной инфраструктуре:

1. Двухфакторная аутентификация пользователей.
2. Антивирусная защита автоматизированных рабочих мест и серверов.
3. Защита почтовых сервисов от фишинга.
4. Защищенный обмен файлами и информацией через файловое хранилище.
5. Обеспечение процесса управления уязвимостями.
6. Реализация парольной политики, соответствующей следующим требованиям:

* длина пароля должна быть не менее 10 символов;
* пароль должен содержать буквы верхнего и нижнего регистра (А-Я, A-Z, а-я, a-z), специальные символы (!, », №, %, \*, /);
* в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов);
* пароли от учетной записи для доступа к собственной инфраструктуре и учетной записи, созданной для доступа к ИТ-инфраструктуре Группы «Т Плюс», должны отличаться.

Приложение №3 к Техническому заданию

на оказание услуг по технической поддержке

системы ITSM на платформе Итилиум

**Форма заявки**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **№ Наряда** | **Описание заявки** | **Дата, время регистрации** | **План. срок решения** | **Факт. срок решения** | **Трудозатраты (ч/час)** |
|  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| **Исполнитель**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ /**  **м.п.** | **Заказчик**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/** **Азизов К.Р /**  **м.п.** |