**Технические характеристики \***

Приобретение ресурсов облачных вычислений, лицензий Microsoft Windows, услуг хранения данных, потоковой передачи данных, доступа в Интернет, межсетевых экранов и сервисов хранения данных.

**Вычислительные ресурсы, включая сертификаты Windows 2022 (или более поздней версии) для виртуальных машин Windows, для указанного количества и виртуальных ЦП.**

| ОС | виртуальный ЦП | ОЗУ, ГБ | Хранилище: 1, Гб | Объем памяти : 2 Гб | Объем памяти : 3,0 ГБ | Сетевые Гбит/сек |
| --- | --- | --- | --- | --- | --- | --- |
| Windows Server Standard 2022+ | 2 | 6 | 100 |  |  | 1+ |
| Windows Server Standard 2022+ | 2 | 6 | 100 |  |  | 1+ |
| Windows Server Standard 2022+ | 2 | 6 | 100 |  |  | 1+ |
| Windows Server Standard 2022+ | 2 | 6 | 100 |  |  | 1+ |
| Windows Server Standard 2022+ | 8 | 48 | 100 | 150 | 2500+ | 1+ |
| Windows Server Standard 2022+ | 8 | 48 | 100 | 150 | 2500+ | 1+ |
| Windows Server Standard 2022+ | 2 | 4 | 100 |  |  | 1+ |
| Windows Server Standard 2022+ | 6 | 24 | 100 |  |  | 1+ |
| Windows Server Standard 2022+ | 6 | 24 | 100 |  |  | 1+ |
| платформа Linux | 2 | 2 | 100 |  |  | 1+ |

**Технические требования к интернет -сервису**

| **Категория** | **Требования** | **Параметр/Метрика** | **Целевое значение / Значение** |
| --- | --- | --- | --- |
| Тип услуги | Доступ в Интернет CIR | Тип услуги | Интернет CIR для бизнеса/предприятий: |
| Тип услуги | Место доставки | Место установки | Стойка CSP DC (Exchange/AD/NGFW) |
| Пропускная способность | Выделенная симметричная полоса пропускания | CIR вверх/вниз | ≥ 100 Мбит/с / 100 Мбит/с, полнодуплексный режим |
| Пропускная способность | Масштабируемость с оплатой по мере использования | Повышение/понижение уровня | Увеличение/уменьшение по запросу выше/ниже 100/100 |
| Пропускная способность | Метод оплаты по факту использования | Учет использования | Простая многоуровневая система оплаты по факту использования (предпочтительно) или 95-й процентиль |
| Пропускная способность | Формирование ниже CIR запрещено. | Формирование/контроль | Ограничение скорости/контроль ниже уровня CIR запрещены (за исключением согласованных мер по смягчению последствий DDoS-атак). |
| Доступность | Доступность услуг | Доступность | ≥ 99,9% в календарный год |
| Доступность | Определение сбоя | Порог потерь | Потеря пакетов ≥ 50% в течение более 1 минуты = сбой в работе сети |
| Обслуживание | Уведомление о плановом техническом обслуживании | Срок уведомления | ≥ 5 рабочих дней |
| Обслуживание | Время проведения планового технического обслуживания | Время суток | Вне рабочего времени (с 00:00 до 06:00 по местному времени) |
| Обслуживание | Ограничение на плановое техническое обслуживание | Итого за месяц | ≤ 8 часов в месяц |
| Производительность | Задержка | 95-й процентиль RTT | ≤ 20 мс до подключения к интернет-провайдеру (восходящий канал/пиринг) |
| Производительность | Дрожь | 95-й процентиль | ≤ 10 мс |
| Производительность | Потеря пакетов | Среднемесячный показатель | ≤ 0,1% (за исключением отключений и технического обслуживания) |
| Пропускная способность | Полезная пропускная способность IP | Goodput против CIR | ≥ 90% CIR |
| Маршрутизация/IP | Публичная IP-адресация | Статическое выделение IPv4-адресов | /29 — публичная подсеть IPv4 (5 доступных IP-адресов) |
| Маршрутизация/IP | Нет оператора NAT | политика NAT | CGNAT не требуется (маршрутизация должна быть общедоступной). |
| Безопасность | защита от DDoS-атак | Объемное снижение | Включено |
| Безопасность | портовый нейтралитет | Разрешенные порты/протоколы | Блокировка необходимых портов исключена. |
| Поддерживать | покрытие NOC | часы работы службы поддержки | 24/7/365 |
| Поддерживать | Время реагирования на неисправность | Ответ | ≤ 15 минут с момента обнаружения/выдачи штрафа |
| Поддерживать | Время восстановления (критическое) | MTTR | Полное отключение/значительное ухудшение качества связи может длиться не более 4 часов. |
| Мониторинг и отчетность | Узнаваемость клиентов | Портал / отчеты | Портал/API или ежемесячный отчет по SLA |
| Лекарственные средства | Сервисные кредиты | График кредитов | Таблица кредитных лимитов |
| Лекарственные средства | Прекращение хронических нарушений | Пункт о выходе | Право на расторжение договора после неоднократных нарушений соглашения об уровне обслуживания (SLA). |

**Требования к лаунчеру следующего поколения (аппаратному обеспечению или соответствующему виртуальному устройству):**

| Спецификация | Класс B |
| --- | --- |
| Типичное использование | Крупный филиал/региональный головной офис (≤500 пользователей, возможность установки нескольких модулей) |
| Пропускная способность FW IMIX (Гбит/с)  измеряется в соответствии с RFC 3511/2647. | ≥8 |
| Предотвращение угроз с использованием полного канала L7 (Гбит/с) | ≥5 |
| Новые сессии в секунду | ≥100 тыс. |
| Максимальное количество одновременных сессий | ≥4М |
| Межсетевой экран с сохранением состояния, NAT, зоны, двойной стек IPv4/IPv6. | Необходимый |
| DPI (L7 App-ID / сигнатура + эвристика) | Необходимый |
| IPS (NGIPS) | Необходимый |
| WAF (интегрированный обратный прокси или тесно интегрированный модуль; набор правил, совместимый с OWASP CRS) | Необходимый |
| Расширенные средства обнаружения вредоносных программ (ML/AV) | Необходимый |
| Песочница | Требуется размещение на территории предприятия. |
| Облачная песочница | Необязательно. Если предлагается: ОБЯЗАТЕЛЬНО шифрование данных при передаче/хранении, предоставление соглашения об обработке данных (DPA), обработка данных в соответствии с GDPR, региональное размещение данных и аттестация по стандартам ISO/IEC 27001/SOC 2 . |
| Расшифровка TLS 1.3 ( прямой прокси и входящий обратный прокси) | Необходимый |
| Концепция нулевого доверия (соответствие стандарту NIST SP 800-207; точка применения политики ZTNA; аутентификация для каждой сессии ) | Необходимый |
| Идентификационная осведомленность (AD/Azure AD/LDAP; сопоставление идентификаторов пользователей) | Необходимый |
| Единый вход для администратора (SAML 2.0 / OpenID Connect) | Необходимый |
| Динамический выбор/управление маршрутом с помощью приложения и SLA (атрибуты MEF 70.1/70.2) | Необходимый |
| Базовая/наложенная сеть. IPsec (ESP) с IKEv2; туннели на основе TLS. | Необходимый |
| Проверка производительности (дрожание/задержка/потери), BFD одношаговый тест | Необходимый |
| MPLS/BGP/OSPF/Static; ECMP | Необходимый |
| Защита VoIP (переключение SIP ALG, сохранение/примечание DSCP) | Необходимый |
| Exchange Online Protection — интеграция с аналогичными системами защиты почты для гибридных потоков. Проверка SPF/DKIM/DMARC; принудительное применение SMTP TLS/ mTLS ; совместимость коннекторов; деактивация вложений; перезапись URL-адресов/эквивалент времени клика; сохранение заголовков/меток времени для отслеживаемости. | Необходимый |
| HA (stateful A/S) | Обязательно; ≤1 с |
| Кластеризация/объединение (единый административный домен, синхронизация политик, унифицированные журналы) | Требуется (≥2 узла) |
| Виртуальные системы (многопользовательские контексты) | Не требуется |
| Медь GE (RJ-45) | ≥12 |
| SFP/SFP+ 1/10G | ≥6 SFP+ |
| 25G SFP28 | Необязательно. Если предлагается: должна обеспечивать совместимость в соответствии со стандартом IEEE 802.3ba/bs. |
| 40/100G (QSFP+/QSFP28) | Необязательно. Если предлагается: должна обеспечивать совместимость в соответствии со стандартом IEEE 802.3ba/bs. |
| Консоль/USB | RJ-45/USB-C |
| Локальный графический интерфейс/интерфейс командной строки; SSHv2; администрирование на основе ролей: | Необходимый |
| API (REST/NETCONF); совместимость с Ansible | Необходимый |
| Передача структурированных Syslog-сообщений (RFC 5424) и Syslog-сообщений с поддержкой TLS (RFC 5425) в SIEM; экспорт в IPFIX или NetFlow (RFC 7011/совместимый). | Необходимый |
| Синхронизация времени NTPv4 | Необходимый |
| SNMPv3 | Необходимый |
| вход переменного тока | 100–240 В переменного тока |
| Вилка/кабель в комплекте | Тип F ( Шуко ) |
| Рабочая температура (°C) | 0…45 |
| Комплект для установки в стойку | Обязательно (1U/2U в зависимости от модели) |
| Уровень шума (дБА при 25°C) | ≤55 |
| Кабель питания | 2× Type-F (при наличии двух блоков питания) |
| Заземляющие принадлежности | Требуется защитное заземление; заземляющие принадлежности входят в комплект (заземляющий кабель/наконечник/винты). |
| Патч-корды | 4× Cat6a (≥2 м) |
| Высокоскоростные межсоединения | В комплект входят 4 ЦАП SFP+ (≤3 м) |
| Включенные лицензии | Подписка на 60 месяцев включает в себя: IPS, фильтрацию URL-адресов, антивирус/антивирусную защиту, идентификацию, SD-WAN, централизованное управление , пересылку журналов, расшифровку TLS/WAF/песочницу. |
| Лицензия песочницы | В стоимость включена лицензия на использование локального движка (60 месяцев ). |
| Поддержка программного обеспечения | Обновления безопасности и выпуск новых функций в течение ≥5 лет с момента приемки. |
| Гарантия на оборудование | Замена NBD в течение ≥3 лет: |
| Документация | Администрирование + руководство по усилению безопасности + справочник по MIB/API |

**Служба передачи данных между Министерством высокотехнологичной промышленности Республики Армения (Вазген Саргсян, 3, Ереван) и ТМК:**

| **Категория** | **Требования** | **Параметр / Метрика** | **Цель / Значение** |
| --- | --- | --- | --- |
| Тип услуги | Сервис L2 "точка-точка" | Тип услуги | Ethernet уровня 2 ( например, EoMPLS / EVPN / эквивалент) |
| Тип услуги | Конечные точки | Конец А / Конец В | Стойка ЦОД CSP (Exchange/AD/NGFW) ↔ Ядро правительственного учреждения ( адрес : Вазген Саргсян, 3, Ереван) |
| Пропускная способность | Выделенная симметричная полоса пропускания | ЦИР | ≥ 100 Мбит/с вверх и вниз, полнодуплексный режим |
| Пропускная способность | Формирование ниже CIR запрещено. | Формирование/контроль | Запрещено формирование/контроль трафика ниже уровня CIR (за исключением согласованной защиты от DoS-атак). |
| Характеристики L2 | кадрирование Ethernet | Стандарт | IEEE 802.3 Ethernet |
| Характеристики L2 | поддержка VLAN | Теги | Поддерживается маркировка VLAN по стандарту IEEE 802.1Q;  QinQ (802.1ad) по запросу. |
| Характеристики L2 | МТУ | Эффективный IP MTU | IP-пакет данных размером ≥ 1500 байт без фрагментации. |
| Избыточность | Разнообразие путей (если указано) | Физические/логические пути | Два разных маршрута и независимый «последний километр» (где это возможно). |
| Доступность | Годовая доступность услуг | Доступность | ≥ 99,9% в календарный год |
| Доступность | Определение недоступности | Порог потерь | Потеря пакетов ≥ 50% в течение более 1 минуты = сбой в работе сети |
| Обслуживание | Уведомление о плановом техническом обслуживании | Срок уведомления | не менее чем за 5 рабочих дней до технического обслуживания |
| Обслуживание | Время проведения планового технического обслуживания | Время суток | Вне рабочего времени ( например , с 00:00 до 06:00 по местному времени) |
| Обслуживание | Ограничение продолжительности технического обслуживания | Итого за месяц | ≤ 8 часов в месяц планового технического обслуживания |
| Задержка | Односторонняя задержка | 95-й процентиль | ≤ 10 мс (офис ↔ CSP) |
| Дрожь | Изменение задержки пакета | 95-й процентиль | ≤ 5 мс |
| Потеря пакетов | Средняя потеря пакетов | Среднемесячный показатель | ≤ 0,1% (за исключением отключений и технического обслуживания) |
| Пропускная способность | Полезная пропускная способность IP | Goodput против CIR | ≥ 90% CIR ( например , полезная нагрузка IP ≥ 90 Мбит/с для услуги 100 Мбит/с) |
| Поддерживать | Время реагирования на неисправность | Ответ | ≤ 15 минут с момента обнаружения или вскрытия билета |
| Поддерживать | Время восстановления – критически важно. | восстановление после отключения электроэнергии | Полное отключение/значительное ухудшение качества связи в рабочее время не должно превышать 4 часов. |
| Поддерживать | Время восстановления - значительное ухудшение | Устранение последствий деградации | Нарушение SLA может занять до 8 часов без полного отключения электроэнергии. |
| QoS | прозрачность DSCP | Обработка DSCP | Сохранять метки DiffServ / DSCP;  не использовать перемаркировку по умолчанию. |
| QoS | 802.1p прозрачность | Биты CoS | CoS 802.1p в помеченных кадрах |
| QoS | Превышение количества заявок ниже CIR не допускается. | Скопление | Отсутствуют обрывы связи, вызванные перегрузкой сети, вплоть до уровня CIR. |
| Мониторинг поставщика услуг | круглосуточное наблюдение | покрытие NOC | Круглосуточный мониторинг состояния каналов связи и метрик. |
| Мониторинг поставщика услуг | Частота зондирования | Интервал зондирования | ≥ 1 зондирование/сек для проверки доступности/потери/задержки/дрожания |
| Мониторинг поставщика услуг | Пороговые значения тревоги – потеря | Триггер потери | Сигнал тревоги срабатывает, если потери превышают 1% в течение более 5 минут подряд. |
| Мониторинг поставщика услуг | Пороговые значения срабатывания сигнализации – задержка | Триггер задержки | Сигнал тревоги срабатывает, если задержка превышает двукратное значение SLA ( например , > 20 мс ) в течение более 5 минут. |
| Мониторинг поставщика услуг | Пороговые значения срабатывания сигнализации – дрожание | Триггер дрожания | Сигнал тревоги срабатывает, если дрожание сигнала превышает двукратное значение SLA ( например , > 10 мс ) в течение более 5 минут. |
| Портал поставщика услуг | Клиентский портал / API | Видимость | Веб-портал или API с отображением статуса практически в режиме реального времени (задержка ≤ 5 мин). |
| Портал поставщика услуг | Сохранение исторических данных | Срок хранения | История данных за период ≥ 365 дней (использование, задержка, дрожание, потери, сбои) |
| Отчетность | Ежемесячные отчеты по соглашениям об уровне обслуживания (SLA) | Объем отчета | Ежемесячный отчет с указанием доступности, задержки, дрожания сигнала, потерь, инцидентов и технического обслуживания. |
| Мониторинг клиентов | Допускаются активные зонды | Транспортный поток зондирования | Клиент может запускать зондирующие запросы ICMP/UDP/TWAMP без блокировки (в разумных пределах). |
| Мониторинг клиентов | Телеметрия CPE | Обмен статистикой | демаркационной станции используется CPE провайдера , то для доступа к базовой статистике интерфейса используется SNMPv3 или телеметрия: |
| Мониторинг клиентов | Предупреждение об использовании – предупреждение | Порог | Предупреждение срабатывает, если уровень CIR превышает 70% в течение более 10 минут. |
| Мониторинг клиентов | Предупреждение об использовании — критическое | Порог | Предупреждение срабатывает, если уровень CIR превышает 90% в течение более 5 минут. |
| Мониторинг клиентов | Предупреждения о качестве | Пороги | Оповещения при потере > 1%, задержке > 10 мс , дрожании > 5 мс в течение > 5 минут. |
| Демаркация | Определение демаркации | Демаркационные точки | границы между сторонами A и B (порты NID/коммутатора) в договоре и документации RFS. |
| Демаркация | Интерфейс передачи | Физический интерфейс | Электрический или оптический Ethernet ( например, 1000BASE-T или 1000BASE-SX/LX или выше) |
| Демаркация | Ответственность за оптику | SFP/SFP+ | Поставщик предоставляет необходимые SFP/SFP+ или медиаконвертеры, если не оговорено иное. |
| Безопасность | Логическая изоляция | VPN / экземпляр | Трафик, передаваемый через выделенный MPLS VPN / EVPN / VPLS или эквивалентный изолированный экземпляр. |
| Безопасность | конфиденциальность полезной нагрузки | Обработка полезной нагрузки | Поставщик услуг не имеет права копировать или проверять полезную нагрузку, за исключением случаев защиты от DDoS-атак или устранения неполадок по запросу. |
| Безопасность | Безопасное управление оборудованием CPE | Протоколы управления | устройствами разграничения сети провайдера используются только защищенные протоколы (SSH, SNMPv3, HTTPS/TLS). |

**Технические требования к сервису хранения данных**

|  |  |  |  |
| --- | --- | --- | --- |
| **Категория** | **Требования** | **Параметр/Метрика** | **Целевое значение / Значение** |
| Резервная копия | Сервис управляемого резервного копирования (производственный) | Объем предоставляемых услуг | Резервное копирование всех виртуальных машин, поддерживающих конфигурации служб, осуществляется поставщиком услуг и обеспечивает согласованность приложений. |
| Резервная копия | Резервный график | РПО | ≤ 24 часов (ежедневное резервное копирование) |
| Резервная копия | Восстановить работоспособность | РТО (цель) | Тест на восстановление доступен по запросу; критическое восстановление ≤ 8 часов. |
| Резервная копия | Удержание | Срок хранения | ≥ 30 дней (базовый период) |
| Резервная копия | Защита резервного хранилища | Неизменность | Неизменяемость или эквивалентная защита от несанкционированного доступа для резервных копий |
| Резервная копия | Резервное шифрование | Шифрование | Шифрование при передаче и хранении |
| Резервная копия | Резервное копирование отчетов | Отчетность | Ежемесячный отчет о резервном копировании (процент успешных резервных копий, защищенные ресурсы, точки восстановления, используемое хранилище). |
| Резервная копия | Оплата по факту использования | модель выставления счетов | Оплата по факту использования на основе защищаемой емкости (ГБ/ТБ) и/или количества защищаемых рабочих нагрузок. |
| Резервная копия | масштабирование по принципу «плати по мере необходимости» | Добавление/удаление защищенных активов | Включение/отключение по запросу для каждого сервера/рабочей нагрузки |
| Резервная копия | Процесс обработки запросов на доступ и восстановление: | Операции | Круглосуточный канал для запросов на восстановление ; восстановление инициируется в течение согласованного времени ответа. |

Подрядчик должен обеспечить предоставление вышеупомянутых услуг и вычислительных ресурсов по модели масштабируемости «по запросу», спроектировав и эксплуатируя систему таким образом, чтобы обеспечить поддержку среднегодового увеличения вычислительной нагрузки не менее чем на 10% без ущерба для качества услуг.

Оплата производится по модели «оплата по факту использования», при условии, что Подрядчик будет предоставлять счет-фактуру за каждый отчетный месяц, включая подробную и прозрачную разбивку фактически использованных вычислительных ресурсов (вычислительные единицы, объемы и другие соответствующие критерии) (подробные требования в разделе «Условия и положения»).

**Требования к Центру обработки данных (ЦОД):**

**Данные центр к требования**

1. Подрядчик предоставляет Заказчику серверы, выделенные для государственного сектора, в инфраструктуре TMC .
2. Инфраструктура TMC должна быть обеспечена системой электроснабжения , которая должна включать как минимум: полностью независимые источники питания (как минимум 2 линии от разных подстанций , которые подключаются к центру обработки данных по разным, не связанным между собой путям), резервные дизель-генераторы, мощность каждого из которых должна быть достаточной и обеспечивать электроснабжение всего центра в случае полного отключения 2 основных источников питания , источники бесперебойного питания (ИБП) с резервным питанием , подсистему автоматического подключения резервных источников, подсистему управления и контроля электроснабжения .
3. Инфраструктура TMC должна быть защищена.по крайней мере два независимыхс системами охлаждения,которые должны как минимум включать системы вентиляции, охлаждения, контроля температуры и влажности для предотвращения загрязнения. Перегрев и отключение. Мощность системы охлаждения должна соответствовать потребляемой мощности , а питание должно подаваться из разных источников.
4. Стабильная температура воздуха в термомеханическом центре должна находиться в диапазоне 20-22 °C (что соответствует диапазону, указанному в стандарте ASHRAE ), а относительная влажность воздуха должна составлять 40-60%.
5. Инфраструктура TMC должна быть обеспечена следующим образом:телекоммуникационная система,которая должна, как минимум, включать и обеспечивать независимые от двух или более провайдеров, непересекающиеся (не имеющие общей точки, без общей опоры ) кабельные каналы с разных направлений, высокоскоростные линии передачи данных, сетевое оборудование, помещение для кросс -соединений и возможность наличия как минимум 3 основных операторов .
6. Подрядчик должен обеспечить выделенный канал связи между офисом или локальным подразделением Заказчика и центром управления технической поддержкой (TMC).
7. Инфраструктура TMC должна быть обеспечена следующим образом:как минимум два **системы** пожарной безопасности, которые должны как минимум включать и обеспечивать подсистему раннего обнаружения дыма, газовую или вакуумную систему. Подсистема пожаротушения , автоматическая система пожарной сигнализации, изоляция кабельных трасс и использование огнестойких материалов. Система пожарной безопасности должна соответствовать стандарту СП 5.13130.2009 ( Системы). из огонь защита . Автоматические системы пожаротушения и сигнализации. Правила проектирования и нормотворчества) и стандарты СП 9.13130.2009 (Пожарная техника. Огнетушители. Требования к эксплуатации) .
8. Инфраструктура TMC должна обеспечивать резервирование N+1 для серверов и их компонентов (например, линий электропередачи ).
9. В случае неисправности, отказа или остановки для технического обслуживания/замены любой основной системы с резервным компонентом, резервная система должна быть активирована и продолжать работать до тех пор, пока основная система не будет восстановлена и не станет работоспособной.
10. Инфраструктура TMC должна быть обеспечена следующим образом:система физической безопасности **,** которая должна включать в себя **:**
    * многоуровневая подсистема контроля и управления доступом ( биометрия , карты доступа и т. д.),
    * Централизованная подсистема управления и регистрации физических входных/выходных данных и окон. Список данных, подлежащих регистрации, должен включать как минимум следующую информацию :
      + Имя и фамилия сотрудника/посетителя.
      + инструмент обеспечения доступности (например, бейдж , биометрическая идентификация) сканирование , карта и т. д.),
      + для идентификации инструментов обеспечения доступности ,
      + конкретный вход/выход, используемый сотрудником/посетителем.
      + человек подтверждающий документ данные ,
      + Дата входа и выхода, час, минута, секунда.
      + примечание о предоставлении или отказе в доступе .
      + В случае отказа – указание причины.
      + вход цель короткий описание .

Зарегистрированные данные должны храниться не менее 90 дней и полностью передаваться Клиенту по запросу.

* + круглосуточного видеонаблюдения должна обеспечивать видеонаблюдение во всех частях ТМК без «слепых» зон. Видеозаписи должны храниться в полном объеме не менее 90 дней. В случае аренды серверного шкафа Заказчику должна быть предоставлена возможность использовать услугу видеонаблюдения в круглосуточном режиме. Срок хранения видеозаписей из серверного шкафа должен быть установлен в соответствии с требованиями Заказчика.
  + Система безопасности должна предусматривать подсистему защиты периметра (ограждения, контрольно-пропускные пункты). турникеты , охранники).
  + обработки данных и его периметр безопасности должны быть оборудованы датчиками , которые будут обнаруживать: движение, несанкционированное открытие дверей и окон, повреждения окон, незапертые двери и окна, а также уведомлять (SMS, электронную почту и т. д.) соответствующих сотрудников.
  + Система безопасности должна позволять переводить центр обработки данных в режим защиты из одной точки. Режим защиты подразумевает инициирование специального рабочего состояния системы безопасности при обнаружении инцидента, угрожающего физической безопасности. В случае активации режима защиты системы безопасности должны быть реализованы как минимум следующие защитные меры:
    - отправка централизованных уведомлений ответственным за реагирование на инциденты (например, группе физической безопасности), руководству и т. д.
    - автоматическая активация дополнительных камер и датчиков .
    - развертывание группы физической безопасности
    - блокирование опасных зон, при условии предварительной оценки.
    - блокировка всех наружных и внутренних дверей без предварительной оценки.
    - обеспечения доступности (например, бейджи , биометрия) Ограничение на использование сканирования , карт и т. д. для небольшой группы сотрудников.
    - некритических операций (например, плановых процессов резервного копирования и архивирования , планового технического обслуживания и тестирования , периодической обработки данных (например, для подготовки аналитических отчетов), работы внутренних и внешних инструментов для совместной работы, доступа к системе для некритического персонала).
  + Система безопасности должна обеспечивать круглосуточный мониторинг и управление **, которые должны как минимум включать в себя: подсистему управления инфраструктурой центра обработки данных, подсистему** мониторинга энергопотребления, температуры охлаждения и влажности , систему обнаружения и предотвращения распространения воды, а также подсистему экстренного оповещения (SMS, электронная почта и т. д.). Мониторинг данные необходимо сохранить​ по меньшей мере три год на определённый период времени ,
  + Исполнитель: его/её С помощью организационных, технических и технологических средств или с привлечением третьей стороны, ТМК должен обеспечивать режим безопасности территории, который должен включать в себя :
    - Порядок посещения ТМК и выполнения работ,
    - процедуры въезда и выезда оборудования.
    - Роли и уровни полномочий сотрудников Заказчика и Подрядчика.
  + Все лица ( сотрудники Подрядчика и Заказчиков), имеющие постоянный и временный доступ (как физический, так и нефизический) к ТМК и его инфраструктуре , должны пройти проверку биографических данных . проверки ), включая …
    - проверка личности ( например, паспортов ) ,
    - Проверка профессиональной пригодности (например, рекомендации или справка с места работы),
    - проверка на наличие судимости (например, судимость и список разыскиваемых лиц).
  + Соответствующим отделом подрядчика. При отсутствии официального разрешения несанкционированному персоналу запрещается входить в служебную инфраструктуру. Однако соответствующим сотрудникам Заказчика разрешается входить в ТМК в чрезвычайных ситуациях, требующих немедленного вмешательства, при соблюдении следующих условий:
    - Заказчик обязан незамедлительно уведомить Подрядчика после начала доступа к ТМК. Право на начало доступа к ТМК и уведомление об этом предоставляется конкретному лицу. Необходимо указать имя, фамилию, паспортные данные, номер телефона и адрес электронной почты последнего .
    - Уполномоченный сотрудник соответствующего отдела подрядчика должен подтвердить вход посредством заявления на получение разрешения в течение максимум 30 минут с момента уведомления о чрезвычайной ситуации. В ходе работ по просьбе Подрядчика к соответствующему сотруднику Заказчика может быть прикреплено сопровождающее лицо.

1. Исполнитель: должен обеспечить, используя собственные организационные, технические и технологические средства или привлекая третью сторону, круглосуточный непрерывный процесс обеспечения информационной безопасности, который должен как минимум включать в себя :
   1. инциденты профилактика , уязвимости поиск , контрмеры означает приложение ,
   2. Круглосуточное наблюдение , кибератаки возможный случаи открытие и анализ настоящий со временем ,
   3. одобренный инциденты реагирование , весь процесс которого должен быть организован в соответствии с международными стандартами и включать следующие этапы: подготовка ( обучение, инструктаж, мониторинг ) , обнаружение, классификация, реагирование, анализ, обработка и отчетность, профилактические меры ( периодические проверки и испытания , модернизация системы и обучение персонала ).
   4. расследования инцидентов в области информационной безопасности . О любом инциденте, произошедшем с критически важными компонентами и повлиявшем на качество предоставляемых услуг, необходимо немедленно сообщить Клиенту, а также предоставить отчет о применении контрмер ( пост- морт). Отчет должен быть предоставлен не позднее чем через 48 часов после применения контрмер.
2. Поставщик услуг должен обеспечить уровень доступности 99,9% (что эквивалентно примерно 8 часам и 45 минутам простоя в год ).
3. Центр обработки данных должен управляться круглосуточно и быть готовым к реагированию на любые инциденты.
4. Центр управления коммуникациями ( TMC) должен обладать надежной сетевой инфраструктурой с резервными сетевыми устройствами , включая маршрутизаторы , коммутаторы и межсетевые экраны .
5. выбрать местоположение TMC. необходимо учитывать и минимизировать потенциальное воздействие наводнений, землетрясений и других факторов окружающей среды.
6. TMC должна иметь возможность предоставлять клиенту выделенную полосу пропускания , отвечающую его требованиям .
7. В системе TMC необходимо предусмотреть автоматическое обнаружение неисправностей или отказов в отдельных компонентах / модулях , предотвращая их эскалацию и распространение на другие части системы.
8. Исполнитель должен иметь следующую сертификацию:
   * Сертификация ISO/IEC 27001
9. Исполнитель, используя собственные организационные, технические и технологические средства или через третье лицо. Необходимо обеспечить, чтобы любая информация Клиента и его носителей обрабатывалась в соответствии с международными стандартами ( например, Руководством NIST 800-88 по очистке носителей информации ) , начиная с установки и заканчивая безопасным уничтожением.
10. Активы исполнителя должны централизованно управляться в соответствии со стандартом ISO/IEC .

**Предоставление услуг**

Исполнитель должен:

1. на портале пользовательский интерфейс для непосредственного управления ресурсами без вмешательства поставщика услуг.
2. Предоставить структурированный и стандартизированный способ создания и управления учетными записями (пользовательскими учетными записями/облачными учетными записями/системными учетными записями), а также возможность просмотра, отслеживания и мониторинга всех ресурсов (данных, сервисов, инфраструктуры) и их потребления.
3. Предоставьте пользователям возможность создавать дополнительных пользователей и предоставлять им доступ к ресурсам. Эта функция также должна быть доступна через пользовательский интерфейс .
4. Обеспечьте неограниченный доступ к пользовательскому интерфейсу с уровнем доступности 99,9% (что эквивалентно примерно 8 часам и 45 минутам простоя в год ) .
5. Предоставьте клиенту полный контроль над его политикой безопасности, включая определение конфиденциальности, целостности и доступности данных и систем.
6. Безопасные пользователи способность определять, применять и управлять политиками доступа .
7. Предоставьте пользователям возможность определять отдельные учетные записи и группы учетных записей с соответствующими правами доступа .
8. Минимизируйте ручной доступ персонала к вычислительным серверам в соответствии с разделом контроля доступа, описанным в стандартах ISO 27001 и ISO 27002 . хосты , хранилище серверы ). Большая часть операций управления вычислительными хостами должна выполняться автоматически ( автоматизированно) . (скрипты ). Действия, выполняемые вручную и автоматически, должны регистрироваться и поддерживаться.в журналах как минимум 90 дней,
9. Услуги, предоставляемые компанией Defender, включая фейерверки ,
10. Предоставьте Клиенту возможность управления определенными службами межсетевого экрана , такими как возможность применения фильтрации по географическому IP-адресу, настраиваемая пользователем служба VPN и другие функции (по запросу Клиента).
11. инструментов управления сетевым трафиком на уровнях OSI 3-7 по всему пути передачи данных клиента.
12. Предоставьте меры по противодействию внешним атакам в соответствии с требованиями OWASP Top 10 (последняя версия ).
13. Предоставить средства противодействия DDoS-атакам.
14. Обеспечьте возможности шифрования данных в хранилищах данных и базах данных.
15. Предоставить услугу управления ключами шифрования, которая позволит Заказчику добавлять, создавать, отслеживать и удалять собственные ключи шифрования в системе управления ключами Подрядчика.
16. Предоставьте ключи доступа ( доступ) ключи ) возможность получать информацию об использовании, заменять старые ключи и удалять неактивные ключи.
17. Обеспечьте долговременную защиту ключей шифрования, предотвращая их потерю или несанкционированное изменение в случае аппаратных сбоев , программных ошибок, сбоев в работе центров обработки данных или других нарушений .
18. Предоставьте гибкие варианты управления ключами шифрования, позволяющие Клиенту выбирать, будет ли Исполнитель управлять ключами шифрования или Клиент возьмет на себя эту ответственность. полный контроль ,
19. Безопасный Клиент к данные полный контроль , как также их сохранение должно быть выполнено Клиент назад заранее согласованный географический в местах ( адресах ),
20. В соответствии с требовать Предоставляем реальные статические IP-адреса/подсети.
21. Разрешать Клиенту использовать собственные IP- адреса , динамические протоколы маршрутизации (BGP, EIGRP, OSPF и т. д.) через ,
22. Осуществлять данные бронировать вариантов Разработка и управление политикой и графиком резервного копирования в соответствии с требовать ,
23. Безопасный Механизм для просмотра и мониторинга платежей за использование ресурсов в режиме реального времени посредством отчетов и визуализаций . Поставщик также должен предоставлять информацию об объеме использования ресурсов и платежах за данный месяц (в согласованные сроки) как в подробном, так и в сводном виде.
24. для сопоставления объемов используемых ресурсов и структуры затрат , а также для прогнозирования будущих затрат.
25. набор инструментов для установки ежемесячных, ежеквартальных и индивидуальных пороговых значений потребления ресурсов для каждого пользователя или группы пользователей , а также для отправки уведомлений при превышении этих пороговых значений , например, по электронной почте или через пользовательский интерфейс . Набор инструментов должен предоставлять предпочтительный вариант. Функция установки пороговых значений и их удобного изменения . Пороговые значения могут быть пропорциональными (в процентах от...). грандиозный всего ), а также с конкретными значениями ( значение ),
26. Предоставляйте информацию об эффективности предоставляемых услуг на основе сравнительного анализа с требованиями, изложенными в данном приложении, посредством отчетов и визуализаций .

**Требования для миграции в среду Performer**

1. Подрядчик обязан предоставить клиенту, использующему собственные локальные или сторонние сервисы, комплект инструментов для миграции сервисов , включающий серверы , базы данных , приложения и другие сервисы, необходимые клиенту.
2. Провайдер не ограничивает типы мигрируемых систем. Различные платформы виртуализации ( например, VMware или её аналоги) эквивалентно : HyperV .) В случае необходимости миграции, клиент заранее информирует является Исполнительскому коллективу электронный по почте , указав миграция предмет система имя и другой необходимый информация.
3. В случае крупномасштабной миграции исполнитель должен предоставить возможности автоматизации миграции, обеспечивающие повторяемость и согласованность операций миграции .
4. Учитывая платформы, являющиеся источником и пунктом назначения миграции ( источник / пункт назначения). платформы ) и официальную документацию по совместимости инструментов миграции. Разработчик должен предоставить инструменты для проверки точности, целостности и совместимости данных после миграции .
5. устаревших систем по требованию клиента , с учетом исходной и целевой платформ миграции ( источник / назначение ) платформы ) и официальную документацию по совместимости инструментов миграции. Подрядчик должен предоставить консультации и предложить соответствующие решения, обеспечивающие работоспособность и совместимость устаревших систем в среде Подрядчика.
6. Подрядчик должен обеспечить возможность масштабирования ресурсов до 200% в соответствии с требованиями Заказчика для обработки рабочей нагрузки во время масштабной миграции (сроки дополнительно согласовываются с Поставщиком).
7. Подрядчик обязан предоставлять услуги по поддержке мигрантов, включая профессиональную ориентацию. и консультация: бесплатно на основе , как также по необходимости в случае технический помощь
8. плановой миграции базы данных Подрядчик должен обеспечить уровень доступности предоставляемых им услуг на уровне 99,9% (что эквивалентно примерно 8 часам и 45 минутам недоступности в год ).
9. Исполнитель должен предоставить централизованный сервис, который позволит Клиенту отслеживать состояние и производительность миграции серверов и приложений в режиме реального времени (например, количество ошибок, исправлений и т. д.).
10. Исполнитель должен предоставить информацию о миграционном статусе, соответствующих критериях и истории миграции. набор инструментов :

**Программа выходит из среды выполнения ( выход). план ) требования**

1. Подрядчик должен предоставить набор инструментов для миграции из своей среды в локальную среду Заказчика или другого поставщика , а также программу выхода ( выход). план ) и услуги, без блокировки в среде исполнителя ( поставщик) блокировка ):
2. Исполнитель должен обеспечить прозрачную и стандартизированную процедуру миграции данных, гарантируя ясность используемых инструментов , API и процессов.
3. Исполнитель обязуется предоставить индивидуальные услуги по поддержке миграции, включая техническую и консультационную поддержку, с учетом конкретных потребностей Заказчика в миграции данных.
4. Исполнитель должен обеспечить бесперебойную миграцию данных.
5. В случае перевода на локальную среду Заказчика или другого поставщика услуг, Исполнитель не должен подавать запросы на дополнительные платежи, помимо тех, которые предусмотрены в положениях договора или иных ограничениях.
6. Исполнитель должен обеспечить экспорт данных в соответствии с форматами и протоколами, указанными Заказчиком .
7. Исполнитель должен предоставить централизованный сервис, с помощью которого Клиент сможет в режиме реального времени отслеживать состояние миграции и производительность своих серверов и приложений (например, количество ошибок, исправлений и т. д.).
8. После завершения миграции Исполнитель должен обеспечить безопасное удаление всех данных Заказчика и, при необходимости, предоставить подтверждающие документы (например, сертификат об уничтожении).

**Обеспечение непрерывности бизнеса , восстановление после катастроф и планы восстановления**

1. Подрядчик обязан иметь план обеспечения непрерывности бизнеса и восстановления после стихийных бедствий (далее именуемый «План»).
2. Исполнитель должен располагать набором инструментов для реагирования на стихийные бедствия и смягчения их последствий .
3. Подрядчик обязан, по меньшей мере, раз в год, внедрять план обеспечения непрерывности бизнеса и восстановления после стихийных бедствий , представляя Заказчику сводный отчет о результатах реализации плана.

План должен включать процедуру реагирования на пандемию . Стратегия смягчения потенциальных последствий может включать наличие резервных групп в разных географических местах для передачи ключевых процессов группам за пределами региона . Список удаленных сотрудников предоставляется заранее и утверждается Заказчиком.

**Дополнительные требования**

* Оборудование, обеспечивающее все вычислительные, информационные и сетевые услуги, должно физически располагаться на территории Республики Армения в течение всего периода предоставления услуг.
* В случае необходимости проведения плановых технических работ, дата и временные рамки выполнения работ должны быть согласованы с заказчиком заранее, не позднее чем за пять рабочих дней.
* Доступность услуг должна составлять не менее 99,9% в год.
* документ (сертификат) , подтверждающий выполнение соответствующего требования или наличие эквивалентного решения , выданный регулирующим органом или признанной на международном уровне организацией в соответствующей области.