# ТЕХНИКАЛЫҚ СИПАТТАМА

**1267857 , Бұлтты серверді жалға алу сатып алу бойынша**
**Ашық тендер тәсілімен**

**Лот № 1 (44 У, 4574282) Әрдайым Интернет желісінде орналасқан серверде ақпаратты физикалық орналастыруға арналған есептеу қуаттарын ұсыну бойынша қызмет көрсетулер**

**Тапсырыс беруші: "Ембімұнайгаз" АҚ**

**Ұйымдастырушы: "Ембімұнайгаз" АҚ**

## 1. ТЖҚ қысқаша сипаттамасы

| Атауы | Мәні |
|---|---|
| Жол нөмірі | 44 У |
| Атауы және қысқаша сипаттамасы | Әрдайым Интернет желісінде орналасқан серверде ақпаратты физикалық орналастыруға арналған есептеу қуаттарын ұсыну бойынша қызмет көрсетулер, Үнемі Интернет желісіндегі серверде жеке ақпарат енгізу үшін есептеуіш қуатпен қамту (хостинг) |
| Қосымша сипаттама | Бұлтты серверді жалға алу |
| Саны | 1.000 |
| Өлшем бірлігі | - |
| Жеткізу орны | ҚАЗАҚСТАН, Атырау облысы, Атырауская область, Г.АТЫРАУ, УЛ.ВАЛИХАНОВА 1 |
| Жеткізу шарттары | - |
| Жеткізу мерзімі | 01.2027 бастап 12.2029 дейін (қоса алғанда) |
| Төлем шарттары | Алдын ала төлем - 0%, Аралық төлем - 100%, Соңғы төлем - 0% |

## 2. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

1. Айқындамалар және қысқартулар

ДӨО Деректерді өңдеу орталығы

Жеткізуші инфрақұрылымы Пайдаланушыларға деректерді сақтауға, өңдеуге және ұсынуға арналған алаң. Серверлік кешендерді, деректерді сақтау кешендерін, сондай-ақ орталықтың жұмыс істеуі және қауіпсіздігін қамтамасыз ету үшін қажетті барлық инженерлік бөлікті қамтиды

ДСЖ Деректерді сақтау жүйесі

Ресурс Деректерді сақтауға арналған есептеу ресурстары, дискілік кеңістіктер (SSD)

VDC Виртуалды дата орталығы, виртуалдандыруға арналған бағдарламалық қамтамасыз етумен басқарылатын бірыңғай қорғалған желіге біріктірілген деректерді сақтауға арналған есептеу ресурстары мен жүйелер кешені

ВЖЖ Виртуалды жеке желі

АҚ Ақпараттық қауіпсіздік

ВМ Виртуальды машина (сервер)

ОЖ Операциялық жүйе

Жұмыс күні 5 күндік жұмыс аптасы кезінде Қазақстан Республикасының аумағында ағымдағы жылы ресми түрде жұмыс күні болып есептелетін күнді білдіреді

Оқиға АТ-қызметінің стандартты жұмыс істеуі шеңберінен шығатын және осы қызметті көрсетуді тоқтата тұрудың немесе сапасын төмендетудің қазіргі немесе ықтимал себебі болып табылатын кез келген оқиға

Проблема Пайда болу себебі белгісіз бір немесе бірнеше байланысты оқиғалар

Қызмет көрсетуге өтінім Гермозонаны қолдауға, ақпарат беруге, консультация беруге немесе оған рұқсат беруге өтінім

Реакция уақыты Техникалық қолдау алу үшін Орындаушыға жүгіну мен Клиенттің туындаған проблемасын шешу бойынша Орындаушы маманының жұмысын бастау арасындағы уақыт кезеңі

Жою уақыты Қызмет көрсетілетін жүйенің жұмыс қабілеттілігін қалпына келтіретін ең ұзақ уақыты.

ДГҚ Дизель–генератор қондырғысы

Виртуальды машина Физикалық жұмыс станциясына ұқсас операциялық жүйелер мен қосымшаларды іске қосатын бағдарламалық жұмыс станциясы

vApp Виртуалды машиналарды мақсаты бойынша біріктіруге (пошта сервері, бухгалтерия және т.б.) және виртуалды машиналар тобын басқаруға мүмкіндік беретін виртуалды машиналар орналастырылған контейнер

АЖ Ақпараттық жүйе

АТ Ақпараттық технологиялар

Проблемалы билет Бірнеше біртекті мәселелер бойынша Service-Desk жүйесінде ашылған өтініш

Штаттан тыс сөндіру Тапсырыс беруші тарапынан алдын ала хабарламай сөндірудің барлық жағдайлары

Авариялық жағдай Виртуалды машинаны, vApp, VDC, VDC инфрақұрылымының бұзылуынан туындаған штаттан тыс сөндіру

Өзіне қызмет ету интерфейсі Бұл бөлінген бұлттық ресурстарды (виртуалды машиналарды, желілерді, сақтау орындарын) дербес басқару үшін Тапсырыс берушіге берілетін веб-портал (басқару панелі). Интерфейс әкімшілік және сервистік операцияларды орындауға, ресурстарды пайдалану мониторингіне және сервистердің жай-күйі туралы ақпарат алуға арналған. Өзіне-өзі қызмет көрсету интерфейсінің жұмыс қабілеттілігі ұсынылатын есептеу және желілік ресурстардың қолжетімділігіне әсер етпейді

СКЖ Сақтық көшірме жүйесі

Firewall Виртуальды желіаралық экран (Firewall)

2. Мақсаты

Осы қызмет көлемі қашықтықтан қол жеткізумен оқшауланған бұлтты орта форматында ұсынылатын виртуалды есептеу ресурстарын жалдау қызметінің (бұдан әрі - Есептеу қуаттарын ұсыну қызметі) құрамын, сипаттамаларын және оған қойылатын талаптарды айқындайды.

Қызмет Тапсырыс берушінің мынадай ақпараттық жүйелерін орналастыруға ұсынылады:

1) SAP S/4HANA;

2) Көлденең мониторинг;

3) Деректерді архивтік сақтау.

Қызметтердің көрсетілу мақсаты — көрсетілген қызметтер көлемі мен техникалық сипаттамаларға сәйкес істен шығуға төзімді, икемді және масштабталатын АТ-инфрақұрылымын қамтамасыз ету.

Осы қызмет көрсету көлемі есептеу ресурстарына, сақтау жүйесіне, желілік инфрақұрылымға, ақпараттық қауіпсіздікке және қызмет көрсету сапасына қойылатын техникалық, функционалдық және пайдалану талаптарын белгілейді.

3. Жалпы талаптар

3.1 Қызмет көрсетілетін орын — Қазақстан Республикасы, Атырау қ.

3.2 Қызмет оқшауланған байланыс арналары арқылы қол жетімді виртуалды есептеу ресурстарының (серверлер, дискілер және желілер) жиынтығын және резервтік көшіру, басқару, техникалық қызмет көрсету сияқты бірқатар қосымша қызметтерді білдіреді

3.3 Қызмет Тапсырыс берушінің АТ қызметтерін ұсынудың үздіксіздігін қамтамасыз ету, АТ инфрақұрылымының икемділігі мен ауқымдылығын арттыру мақсатында ұсынылады

3.4 Қызмет Тапсырыс берушінің ағымдағы инфрақұрылымынан Өнім берушінің инфрақұрылымына Тапсырыс берушінің барлық ақпараттық жүйелерінің толық көшуін қамтиды. Көші-қон Өнім берушінің күшімен және есебінен орындалады және Тапсырыс беруші бастапқы инфрақұрылымға қол жеткізуді ұсынған күннен бастап күнтізбелік 5 (бес) күннен кешіктірмей аяқталады. Көші-қон Тапсырыс берушінің АЖ жұмысын тоқтатпай орындалады. Көші-қон Жеткізушінің инфрақұрылымындағы барлық АЖ жұмыс қабілеттілігі расталғаннан кейін қол қойылатын актіге тараптар қол қойған күннен бастап аяқталды деп есептеледі.

4. ДӨО -на қойылатын талаптар

4.1 ДӨО жеке тұрған күрделі құрылысты (ғимаратты) (бұдан әрі - ДӨО) білдіреді. Ғимарат деректерді өңдеуге және сақтауға арналған жоғары технологиялық жабдықтың жұмыс істеуін қамтамасыз ететін машина залын орналастыру үшін жобаланған және салынған. Объект бөлінген жер учаскесінде орналасқан, бұл тәуелсіздікке және пайдалану қауіпсіздігіне кепілдік береді

4.2 ДӨО тәулік бойы физикалық күзетпен күзетілетін аумақта болуы тиіс. Аумаққа кіру қақпаға қарсы құрылғылармен жабдықталған қақпа арқылы жүзеге асырылуы тиіс. Дата-орталық TIER III деңгейінің талаптарына сәйкес жобалануы және салынуы қажет

4.3 Тапсырыс берушінің инфрақұрылымына инженерлік инфрақұрылымды ажыратпай қызмет көрсету мүмкіндігі үшін ДӨО резервтік компоненттермен жабдықталуы тиіс

4.4 ДӨО -де резервті (АВР) автоматты енгізумен және физикалық бөлек кәбілдік трассалармен 2N схемасы бойынша қоректендіруді толық резервтеуді қамтамасыз ететін екі түрлі трансформаторлық қосалқы станциядан екі тәуелсіз электр қоректендіруі болуы тиіс. Электрмен жабдықтаудың сенімділігіне мынадай талаптар қойылады: - энергиямен жабдықтауды жоғалтқан жағдайда серверлік және желілік жабдық Орындаушының резервтік энергиямен жабдықтауына (ДГУ) автоматты түрде ауысуы тиіс. Энергиямен жабдықтаудың резервтік көзіне ауысу кезінде ұсынылатын сервистің үздіксіздігі бұзылмауы керек

4.5 Кез келген жеке алынған уақыт сәтінде АТ-жүктемесінің жұмысын қамтамасыз ету үшін энергиямен жабдықтау жүйесінің кіру учаскесінің де, механикалық жүйелер үшін де бір тарату арнасының жұмысы жеткілікті

4.6 Резервтік компоненттер мен тарату арналары қандай да бір себеппен пайдаланудан шығарылған кезде, белсенді компоненттердің тұрақты белгіленген қуаты ДӨО жабдығының барлық қажеттіліктерін қамтамасыз ету үшін жеткілікті болуы тиіс

4.7 ДӨО газбен өрт сөндірудің қазіргі заманғы автоматты жүйесімен, қазіргі заманғы климаттық техникамен және электр желісін кепілдендірілген қоректендірудің тоқтаусыз жүйесімен (үздіксіз қоректендіру көздерінің және дизельді электр станциясының болуы) жарақтандырылады

4.8 ДӨО -да сұрау салулар мен оқиғаларға реакцияның уақытын қысқарту үшін аумақта инженерлік жүйелердің мониторингі орталығы және техникалық қолдаудың кезекші мамандары болуы тиіс

4.9 ДӨО 24/7 режимінде объектіні физикалық қорғауды қамтамасыз ететін лицензияланған күзет агенттігінің тәулік бойы күзетінде болуы тиіс

4.10 Объектіде периметрді қорғаудың көп деңгейлі жүйесі іске асырылуы қажет, оның ішінде: сақтау мұрағаты бар ғимараттың периметрі бойынша және ішінде кемінде күнтізбелік 90 (тоқсан) күн бейнебақылау; Периметрдегі қозғалыс және кіру датчиктері; Күзет бекеттеріндегі дабыл түймелері

4.11 ДӨО -тың өтінім бойынша Тапсырыс берушінің қызметкерлерін орналастыру үшін қолжетімді офистік немесе жұмыс үй-жайлары болуы тиіс

4.12 ДӨО ауыр көліктерге арналған кіреберіс және ғимарат бойынша қозғалуға арналған арбалары бар жабдықтарды қабылдау мен түсірудің жеке аймағымен жабдықталуы тиіс

4.13 Тапсырыс берушінің жабдықтарын уақытша сақтау аймағы (кемінде 10 ш.м), күзетілуі және кіруді бақылауы көзделуі тиіс

4.14 ДӨО -да Тапсырыс берушінің жабдықтарын, материалдарын және өзге де активтерін сақтауға арналған жеке қойма орны болуы қажет

4.15 ДӨО -да оны пайдалануға енгізгенге дейін Тапсырыс берушінің жабдықтарын алдын ала тексеруге және баптауға арналған жеке орын (аймақ) болуы тиіс

4.16 Жеткізуші Тапсырыс берушінің АТ-инфрақұрылымын кемінде үш физикалық тәуелсіз деректерді өңдеу орталықтарында орналастыруды көздейтін геоақпаратталған архитектурада орналастыру мүмкіндігін қамтамасыз етуге міндетті Қазақстан Республикасы Үкіметінің 20.12.2016 жылғы № 832 қаулысымен бекітілген, Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптардың 153-тармағының талаптарына сәйкес бір-бірінен қауіпсіз қашықтықта физикалық жағынан алыс орналасқан және Тапсырыс берушінің ақпараттық жүйелерінің істен шығуға төзімділігі мен апатқа төзімділігін қамтамасыз ететін негізгі және 2 резервтік ДӨО -ын (ДӨО) қамтиды. Жеткізуші шартқа қол қойылған сәттен бастап жұмыс екі күн ішінде Орталықтың кемінде үш жеке тұрған ғимаратын иелену немесе жалға алу құқығын растауды ұсынуға міндетті

5. Байланыс арналарына қойылатын талаптар

5.1 Қызметтер көрсету шеңберінде Жеткізуші Тапсырыс берушіге ұсынатын байланыс арналары бойынша талаптар: Жеткізуші екі тәуелсіз байланыс арнасын жеткізушінің орталығынан тапсырыс берушінің мекенжайына дейін ұйымдастыруға тиіс L2, негізгі - 500 мбит/с және резервтік - 200 мбит/с.. Тапсырыс берушінің мекен-жайы: Шоқан Уәлиханов көшесі 1, Атырау қаласы

6. Ресурстарға қойылатын талаптар

6.1 Есептеу ресурстары осы көлемде көрсетілген техникалық талаптарға сәйкес ұсынылады

6.2 Жеткізуші Тапсырыс берушіге жалға алынған ресурстарды орталықтандырылған басқаруды қамтамасыз етуге тиіс

6.3 Тапсырыс берушінің Жеткізуші тарапынан электрондық пошта арқылы электрондық түрде өтінім жіберу арқылы көрсетілетін қызметке техникалық мүмкіндік болған кезде қосымша қуаттарды (процессорлық, дискілік кеңістік, жедел жады) сұратуға құқығы бар, өтінімнен кейін қосымша қуаттарды беру уақыты Жеткізушіде техникалық мүмкіндік болған кезде 2 (екі) жұмыс күнінен аспауы тиіс, ол болмаған кезде - 60 жұмыс күніне дейін

6.4 Есептеуіш ресурстарды пайдалану кезінде Тапсырыс беруші Шартта көрсетілген Тапсырыс берушінің корпоративтік доменінен Жеткізушінің ресми мекенжайына Азайтуға өтінім жіберу арқылы қуаттардың бір бөлігінен (процессорлық, дискілік кеңістік, жедел жады) бас тартуға құқылы. Өтінімде: (i) ресурстар тізбесі және әрбір түр бойынша азайту шамасы; (ii) өзгерістердің күшіне енуінің қалаулы күні; (iii) өткен кезеңдер үшін барлық есептеулердің төленгенін растау. Көлемнің азаюы тараптар қосымша келісімге қол қойған сәттен бастап күшіне енеді

6.5 Тапсырыс беруші есептеу ресурстарын пайдаланудан толық бас тартқан жағдайда, Орындаушы 14 күнтізбелік күн ішінде Орындаушының ресурстарындағы барлық деректерді мұрағаттайды және Тапсырыс берушіге оларды қорғалған арна бойынша көшіріп алу немесе өзінің алынатын тасығыштарына көшіру мүмкіндігін береді. Орындаушы күнтізбелік 30 күн ішінде Тапсырыс берушінің деректерін өз ресурстарынан алып тастамауға міндеттенеді. Бұл ретте Тапсырыс беруші Орындаушының ресурстарында Тапсырыс берушінің ақпаратын сақтау мерзімі ішінде Орындаушы қызметінің құнын төлейді. Деректерді одан әрі Орындаушының келісілген тарифтері бойынша сақтауға болады

6.6 Есептеу ресурстары Жеткізушінің қолданыстағы тарифтері бойынша беріледі. Қосымша қуаттарды беру фактісі Шартқа Қосымша келісіммен тіркеледі, ол ресурстарды пайдалану басталған сәттен бастап 30 (отыз) күн ішінде жасалуға тиіс

7. Функционалға қойылатын талаптар

7.1 ВМ ағымдағы дискілерін «ыстық» кеңейту және жаңа дискілерді қосу мүмкіндігі

7.2 Жалға алынған ресурстар шеңберінде виртуалды машиналардың (жұмыс істейтіндердің де, тоқтағандардың да) жай-күйінің суреттерін жасау мүмкіндігі

7.3 Қажетті параметрлерді (vCPU, RAM, NVMe, ОС және т.б.) көрсете отырып, виртуалды машиналарды (ВМ) жасау және жою; Интерфейс арқылы ВМ қосу, ажырату, қайта қосу және тоқтату; ВМ конфигурациясын өзгерту: виртуалды процессорлар санын өзгерту (vCPU); жедел жады (RAM) көлемінің өзгеруі; виртуалды дискілерді қосу, жою және өзгерту; желілік адаптерлерді өзгерту және оларды виртуалды желілерге байланыстыру; Ұсынылған үлгілер (VM templates/vApp templates) немесе ISO-бейнелер негізінде операциялық жүйелер мен қосымшаларды таңдау және орнату; Меншікті ISO-бейнелер мен ВМ үлгілерін виртуалды ұйымға импорттау; Тапсырыс берушінің желілік кеңістігін жүйенің басқа пайдаланушыларынан оқшаулау (tenant isolation); Виртуалды желілерді дербес құру және жою (Org VDC networks); Виртуалды маршрутизатор деңгейінде фаерволдарды, NAT, маршруттарды және ВЖЖ баптау

7.4 СКЖ-не қойылатын талаптар: Жүйе өзгертілген блоктарды қадағалау технологиясын пайдалана отырып, инкрементальды көшіруді қолдайтын виртуалды машиналарды резервтік көшіруді қамтамасыз етуі тиіс.

Кесте бойынша саясатты және сақтау мерзімі саясатын құру мүмкіндігімен резервтік көшіру, қалпына келтіру және репликалау тапсырмаларын орталықтандырылған басқаруды қамтамасыз ету қажет.

Жүйе резервтік көшірмелердің бүтіндігін және қалпына келтіру мүмкіндігін автоматты түрде тексеруді қолдауға тиіс.

Сақтық көшірмелерді сақтау орны сақтауды баптау деңгейінде дедупликациялауды, қысуды, сондай-ақ жоюдан қорғауды (immutable backup) қолдауы тиіс. Барлық аса маңызды деректердің резервтік көшірмелері өнімді деректер үшін пайдаланылатын негізгі деректерден физикалық бөлінген бөлінген деректерді сақтау жүйесіне (ДСЖ) орындалуы тиіс. Резервтік көшірмелерді негізгі деректер сияқты сол ДСЖ-не орналастыруға жол берілмейді. Орындаушы дерекқорларды, жүйелерді және виртуалды машиналарды таспалық кітапханаларға немесе дискілік массивтерге резервтік көшіру мүмкіндігін қамтамасыз етеді. 13,1-тармақта көрсетілген көлемде деректерді сақтау және келісілген кесте бойынша резервтік көшіру операцияларын орындауды, резервтік көшіру үшін БҚ ұсынуды қоса алғанда, осы тармақта сипатталған қызметтер Шарт бойынша қызметтердің құнына кіреді.

7.5 Орындаушы танымал операциялық жүйелердің бейнелер каталогын қамтамасыз етеді. Операциялық жүйенің қажетті бейнесі немесе операциялық жүйе жүйесінің нұсқасы болмаған жағдайда, Тапсырыс беруші Орындаушыны қосымша бейнелерді жүктеу қажеттілігі туралы хабарлайды

7.6 Орындаушы кейіннен каталогта жариялау үшін Тапсырыс берушіден сурет сұратуға құқылы

7.7 Орындаушы, егер осы бейне ҚР Заңнамасын бұзса және/немесе АТ инфрақұрылымының қауіпсіздігі үшін әлеуетті қатері болса (оның ішінде өндіруші немесе қоғамдастық тарапынан қолдау циклі аяқталған майнингке, бұзуға немесе ескірген өнімдерге арналған БҚ), бейнені каталогқа орналастырудан бас тартуға құқылы

7.8 Тапсырыс берушімен келісілгеннен кейін баламалы гипервизорларды, пайдалануға жол беріледі

7.9 Стандартты сәулет x86 серверлерінде жұмыс істейтін 32 және 64-биттік қонақ НЖ қолдау

8. Физикалық және ақпараттық қауіпсіздікке қойылатын талаптар

8.1 Жеткізуші Тапсырыс беруші үшін Орталықта орналастырылған оның барлық деректерінің құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етеді

8.2 Жеткізуші Қызмет шеңберінде Тапсырыс берушінің резервтік көшірмелерін, виртуалды машиналарының бейнелерін және деректерін басқа Орталыққа көшіру (көшіру) мүмкіндігін қамтамасыз етеді (Тапсырыс берушінің талабы бойынша). Ауыстыруды (көшіруді) Тапсырыс беруші Шарттың құнын ұлғайтпай осы Қызмет шеңберінде дербес жүзеге асырады. Тапсырыс беруші виртуалды машиналар мен деректер бейнелерінің толық көші-қонын растағаннан кейін Жеткізуші жою фактісінің құжаттамалық дәлелдемелерін ұсына отырып, Тапсырыс берушінің барлық деректерін жоюға міндеттенеді

8.3 Жеткізуші Тапсырыс берушіге бөлінген шекте виртуалды ресурстарды оқшаулауға кепілдік беруге міндеттенеді

8.4 Жеткізуші ДӨО жабдығына бөгде адамдардың физикалық қолжетімділігін шектеуді қамтамасыз етеді

9. Техникалық қолдауға қойылатын талаптар

9.1 Тәулік бойы кепілдендірілген техникалық қолдау Қызметтер бірыңғай техникалық қолдау қызметі арқылы телефон қоңыраулары (телефон желісі Тапсырыс берушінің кіріс қоңыраулары үшін әрқашан қолжетімді болады) және электрондық пошта арқылы Қызмет көрсетудің бүкіл мерзімі ішінде Тапсырыс берушінің өтінімдерін тіркеу және өңдеу үшін әрқашан қолжетімді болады

9.2 Жеткізуші жауапты тұлғаларды (техникалық мамандарды) көрсете отырып, өтініштерді тіркеу үшін техникалық қолдау қызметінің байланыс деректерін ұсынады

9.3 Жеткізушінің Техникалық қолдау қызметі үздіксіз режимде жұмыс істейтін болады: «тәулігіне 24 (жиырма төрт) сағат, аптасына 7 (жеті) күн» Қызмет көрсетудің барлық мерзімі ішінде демалыс және мереке күндерін қоса алғанда

9.4 Тапсырыс беруші Қызмет жұмысында Инцидент пен авариялық жағдайды анықтаған жағдайда, Тапсырыс беруші техникалық қолдау қызметін Инциденттің бар екендігі туралы хабардар етеді. Инцидент туралы ақпарат Тапсырыс берушінің келісімі бойынша телефон (тар) арқылы немесе электрондық пошта арқылы не өзге де тәсілмен беріледі

9.5 Жеткізуші тарапынан қызметті уақытша ажыратуды талап ететін жұмыстар жұмыстан тыс уақытта немесе демалыс және мереке күндері жүргізілуге тиіс. Жеткізуші тапсырыс берушіні кемінде 3 (үш) жұмыс күні бұрын ресми хатпен хабардар етуге және жұмыстарды жүргізу басталғанға дейін Тапсырыс берушіден жазбаша келісім алуға тиіс

9.6 Анықталған мәселе бойынша Клиенттің сұрауына жауап беру уақыты жұмыс уақытында 15 минуттан және жұмыс істемейтін уақытта 45 минуттан аспауы тиіс, ал ірі зақымдарды жою 2 (екі) сағаттан аспауы тиіс. Өнім беруші Тапсырыс берушіге тіркелген оқиғаның нөмірі, оқиғаның қысқаша сипаттамасы бар оқиғаны тіркеу уақыты туралы хабарлайды.

9.7 Жеткізуші инфрақұрылымның барлық оқиғаларын (виртуалды, желілік және т.б.) журналға түсіруді қамтамасыз етуге және Тапсырыс берушінің ресми өтінімі бойынша оқиғалар журналына қол жеткізуді ұсынуға міндеттенеді

9.8 Авариялық жағдайлар немесе Қызметтерді көрсетуде үзілістер болған жағдайда, Авторландырылған пайдаланушы тосын оқиғаны Тапсырыс берушілердің сүйемелдеу қызметінде тіркейді. Бос тұру тосын оқиға тіркелген сәттен бастап Қызметті қайта бастау туралы хабарламаға дейін есептеледі. Авариялық жағдай деп шартта көзделген қызмет көрсетуді тоқтатуға байланысты қандай да бір кіші жүйе орындайтын процестің авариялық аяқталуы түсініледі. Жүйе жұмысы кезінде жүйе жұмысының сенімділігіне әсер ететін мынадай авариялық жағдайлар болуы мүмкін: - базасында VDC алаңы салынған серверлік және желілік жабдықтың электрмен жабдықтаудағы істен шығуы; - Гермозона инфрақұрылымын электрмен жабдықтаудағы ақау; - VDC алаңының бағдарламалық-аппараттық кешенінің жұмысындағы іркілістер. Істен шығу тапсырыс беруші жүйесінің жұмысқа қабілеттілігінің болмауына алып келген жағдайларда қолжетімсіздік уақыты инцидент тіркелген сәттен бастап есептеледі

9.9 Сұрауларды, проблемаларды, өтінімдерді өңдеу циклі барлық сұраулар тіркелетіндей және бірде-бір проблема шешілмейтіндей етіп құрылуы тиіс. Тапсырыс берушіге өтінішті өңдеу мәртебесінің және проблема мәртебесінің өзгергені туралы хабарланады

9.10 Бір жабдықтың (сервердің, желілік жабдықтың, қауіпсіздік жабдығының) істен шығуы сервистің тоқтауына алып келмеуі тиіс; Жеткізушінің инфрақұрылымы сапалы және үздіксіз қызмет көрсету үшін істен шығуға төзімді және сенімді болуы тиіс

9.11 Жеткізуші Орталықтың істен шығуға төзімділік коэффициентін кемінде 99,9% қамтамасыз етуі қажет

9.12 Жеткізушінің Тапсырыс берушіден ақауларды жою мәніне және т.б. электрондық пошта, телефон байланысы арқылы келіп түсетін өтінімдерді қабылдайтын және Тапсырыс берушіге қатысты хабарламаларды электрондық пошта, телефон байланысы арқылы жіберетін тәулік бойғы негізде техникалық қолдаудың жедел қызметі болуға міндетті

9.13 Жеткізуші Шарт жасалған күннен бастап 2 (екі) жұмыс күні ішінде Тапсырыс берушінің АЖ орналастыру үшін осы техникалық ерекшелікте көрсетілген көлемге сәйкес ресурстардың болуын және қол жетімділігін растауға тиіс

9.14 Жеткізуші Шарт жасалған күннен бастап 2 (екі) жұмыс күні ішінде орналасқан мекенжайын көрсете отырып, негізгі Орталықтың және 2 резервтік Орталықтың болуы туралы хатты ұсынуы керек

9.15 Қызметтің жұмыс істеу режимі аптасына 7 күн 24 сағат сақталуы тиіс

9.16 Орындаушы авариялық жағдайларда VDC жұмыс қабілеттілігі мен қалпына келтіру уақытына кепілдік береді

9.17 Сондай-ақ Тапсырыс берушінің сұрау салуы бойынша Орындаушы резервтік Орталықта қалпына келтіру жоспарын әзірлей және ұсына алады

9.18 Орындаушыны техникалық қолдау қызметінің процестері тиісті Service desk жүйесіне қолдау көрсетілуі тиіс

9.19 Жеткізушінің инфрақұрылымы жаппай зақымданған жағдайда жою мерзімі авариялық-қалпына келтіру жұмыстарының барысы туралы сағаттық есепті ұсына отырып, Тапсырыс берушінің дәлелді келісімі бойынша ғана 2 (екі) сағаттан аспайтын мерзімге ұзартылуы мүмкін

9.20 Жаппай зақымдану - бұл кейіннен логтарда немесе Проблемалық билетті ашуда расталған бірыңғай проблемасы бар Service Desk ДБ-да бірнеше жекелеген өтінімдер

9.21 Тапсырыс беруші өзіне бөлінген тұтынылатын ресурстарды тапсырыс берушінің қаражатымен көру мүмкіндігіне ие болуы тиіс

9.22 Орындаушы Тапсырыс берушінің сұрау салуы бойынша пайдаланылатын жабдықты виртуалдандыру деңгейінде және ДӨО -да егжей-тегжейлі көрсетуге міндеттенеді

9.23 Кешенді оқыс оқиғалар туындаған кезде Инфрақұрылымды жеткізуші Тапсырыс берушінің сұратуы бойынша қолданбалы БҚ-ны сүйемелдеу бойынша Тапсырыс берушінің басқа мердігерін тарта отырып, кезекші инженердің бірлескен жұмыс топтарына қатысуын қамтамасыз етуге, сондай-ақ Тапсырыс берушінің сұратуы бойынша Тапсырыс берушінің сұратуы бойынша 2 сағаттан аспайтын мерзімде виртуалдандыру платформасының, ДСЖ және Қызмет көрсетуге тартылған желілердің логтарын ұсынуға міндетті

10. Серверлік жабдыққа, деректерді сақтау жүйесіне және желілік жабдыққа қойылатын техникалық талаптар

10.1 Серверлік жабдық: Серверлік жабдық мынадай талаптарға жауап беруі тиіс. Архитектура: қазіргі заманғы x86-64 серверлік процессорлар базасында кемінде екі сокет. Процессорлар: 4-ші буындағы серверлік процессорлар деңгейінен төмен емес, тактілік жиілігі 2,8 ГГц-ден төмен емес әрбір процессорға кемінде 32 физикалық ядро. Жады: 5600 MT/s кем емес тиімді жиілікпен DDR5 кем емес жедел жады қолдау, қателерді түзету функциясы бар модульдерді орнату мүмкіндігі (ECC). Серверге орнатылған жедел жадының жалпы көлемі - одан әрі кеңейту мүмкіндігімен кемінде 2000 ГБ. Желілік интерфейстер: әрқайсысы 25 Гбит/с кем емес жылдамдықтағы екі порты бар, виртуалдандыру енгізу-шығару технологияларын (SR-IOV, VLAN, VXLAN) қолдайтын кемінде екі адаптердің болуы. Аппараттық мониторингті, қашықтан басқаруды және out-of-band-қолжетімділікті қолдау (мысалы, IPMI немесе ұқсас). Серверлік жабдық SAP HANA (Tailored Data Center Integration немесе Certified Solution) бағдарламасымен жұмыс істеу үшін сертификатталуы тиіс. Жабдықты сертификаттау (Tailored Data Center Integration немесе Certified Solution) SAP қолдау порталында жариялануы тиіс

10.2 Деректерді сақтау жүйесі (ДСЖ): Пайдаланылатын деректерді сақтау жүйесінде мыналар болуы керек: Контроллерлерді толық резервтеу (HA конфигурациясы); әрбір порттың өткізу қабілеті кемінде 25 ГБ/с (секундына гигабит); кем дегенде екі диск істен шыққан кезде ақауларға төзімділікті қамтамасыз ететін RAID DP немесе баламалы технологияны қолдау, Spare Disk болуы; қайталануды, қысуды және жұқа провизияны қоса алғанда, дискілік кеңістікті тиімді пайдалану технологиясы; NVMe SSD дискілері, жоғары жүктелген IOPS сценарийлері үшін оңтайландырылған; iSCSI, NFS, S3 және SMB протоколдарын қолдау. Деректерді сақтау жүйесі SAP HANA (Tailored Data Center Integration немесе Certified Solution) бойынша жұмыс істеу үшін сертификатталуы тиіс. Жабдықты сертификаттау SAP қолдау порталында жариялануы керек

10.3 Сақтық көшірме жасау үшін деректерді сақтау жүйесі: пайдаланылатын деректерді сақтау жүйесінде: контроллерлерді толық резервтеу (HA конфигурациясы); әрбір порттың өткізу қабілеті кемінде 25 Гб/с (секундына гигабит); RAID DP немесе кемінде екі дискінің істен шығуы кезінде ақауларға төзімділікті қамтамасыз ететін баламалы технологияларды қолдау; NL дискілер; iSCSI протоколдарын қолдау.

10.4 Желілік жабдық: коммутациялық жабдық мыналарды қамтамасыз етуі керек: біріктіруді қолдайтын (LACP) кемінде 48 25GbE порты (SFP28); кемінде 8 санында 100GbE (QSFP28) порттары бар; қуат пен желдету резервінің болуы; RoCEv2, LLDP, LACP, BGP, ЕВЖЖ және VXLAN протоколдарымен үйлесімділік; сегменттеуді қолдау және VLAN; функционалдылықты орнату кезінде қате болған жағдайда кері қайтаруға болатындай конфигурацияны қолданудың транзакциялық тәсіліне қолдау көрсетілуі керек; Қолмен расталмаған жағдайда конфигурацияны қолдану транзакциясын автоматты түрде қайтару механизмін қолдау

11. SAP ішкі жүйесімен үйлесімді сертификатталған ОЖ ға қойылатын талап

11.1 Жалпы талаптар: Операциялық жүйе: ұзақ мерзімді қолдау және SAP-пен дәлелденген үйлесімділігі бар корпоративтік Linux дистрибутиві; Linux ядросы 4.12-ден төмен емес, 4.18 және одан жоғары нұсқасы ұсынылады; пакет менеджері: тәуелділікті шешу жүйесі бар RPM пакеттерін қолдау; негізгі файлдық жүйе: EXT3, EXT4, XFS немесе Btrfs; оңтайлы жұмыс істеу үшін Параметрлер Файлдық жүйелері бар SAP (мысалы, SAP жұмыс каталогтары үшін "noatime" атрибутын өшіру); бөлім өлшемдері SAP талаптарына сәйкес келуі керек, соның ішінде журналдар, уақытша файлдар және сақтық көшірмелер үшін арнайы орын; SAP жұмысын жақсарту үшін ядро параметрлерін орнату; стандартты Linux құралдары мен мамандандырылған SAP утилиталарын қолдана отырып өнімділікті бақылау; келісімшарттың жарамдылық мерзіміне ресми техникалық қолдау көрсету; қауіпсіздік пен түзетулердің тұрақты жаңартуларын қосу

12. Виртуалды желіаралық экранға (firewall) қойылатын талаптар

12.1 Жалпы талаптар: Пайдаланушылардың шектелмеген санына лицензиялау. Жеткізілетін лицензияның құрамына виртуалды желіаралық экран (firewall) өндірушісінен Есептеу қуаттарын ұсыну қызметін көрсетудің барлық кезеңінде 24/7 режимінде ресми тікелей техникалық қолдау кіруі тиіс. Қолдау мыналарды қамтуы тиіс:

• Жаңартуларға, консультацияларға және өтініштерді тіркеуге қол жеткізу.

• Қауіпсіздік модульдерінің сигнатураларын және қауіп-қатерлер тізбесін үнемі автоматты түрде жаңарту.

Виртуалды желіаралық экран (firewall) жетекші виртуалдандыру платформаларында: VMware ESXi, Microsoft Hyper-V, KVM, Xen орнату және сүйемелдеу мүмкіндігіне ие болуы тиіс

12.2 Функционалдық мүмкіндіктері: IP, порттар, қосымшалар бойынша сүзгілеумен желіаралық экрандауды қолдау. Өткізу жолағын басқару (Traffic Shaping) және жүктеме теңгерімі. NAT, PAT, саясатқа негізделген бағыттауды қолдау, VLAN tagging (802.1Q). hub-and-spoke топологияларын және IKE сертификаттары бойынша аутентификацияны қоса алғанда, ВЖЖ-ті (PPTP, IPSec, SSL) ішкі қолдау. Сигнатураларды автоматты түрде жаңарту және пайдаланушы ережелерін баптау мүмкіндігі. ICAP хаттамасы арқылы біріктірілген SSL трафигін инспекциялау. Бағдарламаларды бақылау, DoS-тен қорғау, URL, сайт санаттары және MIME тақырыптары бойынша сүзу. Вирусқа қарсы қорғау, антиспам-сүзу, DLP (деректердің жылыстауын болдырмау) функциялары. SD-WAN және WAN қосылыстарын оңтайландыруды қолдау. Web-интерфейс және CLI арқылы басқару мүмкіндігі, журналға жазуды және SIEM-жүйелермен интеграцияны қолдау

12.3 Пайдаланушыларды қолдау және аутентификация: Ішкі база, Active Directory, RADIUS/LDAP, IP/MAC, топтық саясат арқылы аутентификация. Рөлдерді шектеумен әкімшілендірудің көп деңгейлі моделі

12.4 Ресурстық параметрлер: бір виртуалды желіаралық экранды маршрутизациясы бөлек және қауіпсіздік саясаттары тәуелсіз кемінде 10 (он) логикалық тәуелсіз виртуалды құрылғыға бөлуді қолдау, кемінде 10 (он) виртуалды желілік интерфейс, кемінде 2 (екі) ядро (vCPU), кемінде 2 (екі) ГБ виртуалды жедел жад (vRAM) және 32 (отыз екі) ГБ локалды сақтау орны. Кемінде 10 000 (он мың) трафикті сүзу ережесін қолдау.

Қауіпсіздікті базалық тексерулер кешені (IPS және SSL/TLS инспекциясы) қосулы кездегі өткізу қабілеті: кемінде 500 Мбит/с (тапсырыс берушінің интернет-арнасының өткізу қабілетіне сәйкес)

12.5 Сервистерге жазылу: Негізгі сервистерге белсенді жазылудың болуы: IPS, антивирус, антиспам, web-контентті сүзу, бұлтты құмсалғыш (cloud sandbox)

13. Ұсынылатын есептеу ресурстарының көлеміне қойылатын талаптар

vCPU виртуалды процессоры бір vCPU-ға бір ГГц жиілігі есебінен көрсетілген. Виртуалды машинаны жасау кезінде кемінде 64 vCPU және кемінде 200 ГБ жедел жады бөлу мүмкіндігі болуы тиіс.

13.1. Шарт бойынша жиынтық көлем

| № | Өнім | Өлшем бірлігі | Саны |
|---|---|---|---|
| 1 | Виртуалды vCPU процессоры | Ghz | 1 792 |
| 2 | vRAM виртуалды жады | GB | 5 316 |
| 3 | SSD NVMe дискілік кеңістігін ұсыну | GB | 111 598 |
| 4 | Кем дегенде 10K жылдамдығымен дискілік кеңістікті немесе баламалы технологияны ұсыну | GB | 117 256 |
| 5 | Сақтық көшірме жүйесі | VM | 72 |
| 6 | Виртуалды желіаралық экран (Firewall) | Лицензиялар | 1 |
| 7 | SAP серверлеріне арналған ОЖ | Лицензиялар | 14 |

8 Ортақ мақсаттағы серверлерге арналған ОЖ Лицензиялар 15

9 Сақтық көшірмені басқару Ай 36

10 Виртуалды желіаралық экранды басқару (Firewall) Ай 36

11 Байланыс арнасын жалға беру L2ВЖЖ (Негізгі) Мбит/с 500

12 Байланыс арнасын жалға беру L2ВЖЖ (Резервтік) Мбит/с 200

14. Резервтік көшіруге және авариялық қалпына келтіруге қойылатын талаптар

14.1 • Жеткізуші резервтік көшіруді және инфрақұрылымдық деңгейде қалпына келтіруді қамтамасыз етеді: виртуалды машиналар (ВМ), виртуалды дискілер (NVMe/SSD), vApp конфигурациялары, виртуалды желілер параметрлері және Firewall ережелері.

• Жеткізуші резервтік көшіру жүйесінің платформингін (СКЖ) - БҚ, виртуалдандыру агенттерін, бэкап және деректерді берудің оқшауланған арналарына бөлінген ДСЖ ұсынады және қызмет көрсетеді.

• Жеткізуші консистенттік түсірілімдерді (Application-Consistent Snapshots) орындаудың техникалық мүмкіндігін қамтамасыз етеді және Тапсырыс берушімен және/немесе қолданбалы бағдарламалық қамтамасыз ету мен ББАЖ-ды басқаратын үшінші тұлғалармен өзара іс-қимыл жасау үшін СКЖ интерфейстерін/құралдарын ұсынады.

• Резервтік көшіру Тапсырыс берушімен келісілген Резервтік көшіру жоспарына сәйкес жүзеге асырылады. Резервтік көшіру көлемі Техникалық ерекшеліктің 13.1-тармағынан аспауы тиіс.

14.2 Үздіксіздіктің инфрақұрылымдық өлшемдері (RPO және RTO)

Жеткізуші виртуалдандыру платформасы мен ДСЖ деңгейінде мынадай көрсеткіштердің сақталуына кепілдік береді:

• Өнімді инфрақұрылым үшін (SAP S/4HANA-ға арналған ВМ және Көлденең мониторинг):

o Инфрақұрылымдық RPO (Recovery Point Objective): толық түрде ЖМ үшін 24 сағаттан артық емес;

o Инфрақұрылымдық RTO (Recovery Time Objective): резервтік көшіру жоспар-кестесінде келісіледі.

• Критикалық емес және мұрағаттық ВМ үшін:

o RPO: 24 сағаттан артық емес;

o RTO: резервтік көшіру жоспар-кестесінде келісіледі.

• Жеткізуші резервтік көшіру үшін дискілік кеңістіктің бөлінген көлемі шеңберінде Тапсырыс берушінің резервтік көшіру жоспарына сәйкес виртуалды машиналарды резервтік көшіруді ұйымдастыруға міндеттенеді. Толық, инкрементальды резервтік көшіру мүмкіндігі.

14.3 СКЖ деректерін әкімшілендіру және қорғау

• Жеткізуші Тапсырыс берушімен бекітілген кестеге сәйкес ВМ резервтік көшіру процестерін ұйымдастырады және тәулік бойы сүйемелдейді.

• Резервтік көшірмелер өнімді дискілік массивтерден физикалық және логикалық оқшауланған жеке АШҚ-да орналастырылады.

• Жеткізуші резервтік көшірмелерді сақтау орнын рұқсатсыз жоюдан, қайта жазудан және шифрлаудан (Immutable Backup/WORM технологиясы) қорғауды қамтамасыз етеді.

14.4 Бақылау қалпына келтіру және верификация (Sandbox Testing)

• Жеткізуші резервтік көшірмелердің бақылау сомаларының тұтастығын күнделікті автоматты бақылауды қамтамасыз етеді.

• Жеткізуші ай сайын Тапсырыс берушінің кездейсоқ таңдалған ЖМ/дискілерін операциялық жүйенің сәтті жүктелуін және виртуалды дискілердің қол жетімділігін тексере отырып, оқшауланған тест сегментіне (Sandbox) тестілік бақылау айналдыруды жүргізуге міндетті.

• Жүргізілген тексерулер мен сынақтан өткізіп қалпына келтіру нәтижелері СРК-ның ай сайынғы есебіне енгізіледі. Бұл есеп Тапсырыс берушіге беріледі.

14.5 Мониторинг және техникалық өзара іс-қимыл

• Жеткізуші СКЖ тапсырмаларының жай-күйіне тәулік бойы (24/7) мониторинг жүргізеді. Ақау болған жағдайда Жеткізуші 2 (екі) сағат ішінде ақаудың инфрақұрылымдық себебін жоюға және көшіруді қайта іске қосуға міндетті.

• Жүйелерді қалпына келтіру жөніндегі жұмыстарды жүргізу кезінде • Жеткізуші Тапсырыс берушінің мамандарымен және қолданбалы АЖ бойынша мердігерлермен жедел-техникалық өзара іс-қимыл жасау үшін кезекші инженерді бөледі.

15. Firewall әкімшілігіне қойылатын талаптар

15.1 Жалпы талаптар: Өнім беруші Тапсырыс берушінің сұранысы бойынша виртуалды желілік экранды (Firewall) (бұдан әрі – Firewall) әкімшілендіру бойынша техникалық жәрдем көрсетуді жүзеге асырады.

Firewall-ды әкімшілендіруге жәрдемдесу Тапсырыс беруші ұйымдастырған VPN-қосылым арқылы немесе тек Firewall-ға дейін шектеулі қолжетімділігі бар VDC панелі арқылы орындалады. Тапсырыс беруші Firewall-ға қосылу үшін есептік жазбаны жасайды және Өнім берушіге береді.

Техникалық жәрдем көрсету шеңберінде Өнім беруші Тапсырыс берушінің сұранысы бойынша мыналарды орындайды:

• Firewall-да желілік интерфейстерді жасау, өзгерту, жою;

• Тапсырыс берушінің №4 қосымша нысаны бойынша сұранысы (бұдан әрі – Сұраныс) негізінде Firewall саясаттарын жасау, өзгерту, жою;

• Firewall-ды жаңарту;

• Firewall конфигурациясының резервтік көшірмесін жасау.

15.2 Сұранысты жіберу және орындау тәртібі: Тапсырыс беруші сұранысты Өнім берушінің электрондық поштасына жібереді. Өнім беруші сұраныстарды жұмыс уақытында: сағат 08:30-дан 18:00-ге дейін өңдейді және орындайды. Firewall-дағы маңызды (критикалық) трафиктің бұғатталуына байланысты авариялық сұраныстар Жоғары басымдық үшін белгіленген мерзімдерде (№1 қосымша) тәулік бойы (24/7/365) режимінде өңделеді және орындалады. Firewall-ды қайта жүктеу немесе жаңарту қажет болған жағдайда, жұмыстарды орындау уақыты Тапсырыс берушімен алдын ала, бірақ Өнім берушінің жұмыс уақыты аралығында келісілуге тиіс (АЖ қолжетімділігін қалпына келтіру үшін шұғыл қайта жүктеуді талап ететін авариялық жағдайларды қоспағанда).

Жұмыс уақытынан тыс уақытта түскен жоспарлы сұраныстар келесі жұмыс кезеңінде өңделуге және орындалуға тиіс.

Сұраныстарды өңдеу және орындау мерзімін Өнім беруші күрделілігіне қарай анықтайды және ол 2 (екі) сағаттан 1 (бір) жұмыс күніне дейінгі уақытты құрайды.

Тапсырыс беруші толық емес немесе бұрыс (қате) ақпарат ұсынған жағдайда, Өнім беруші қосымша мәліметтерді сұратуға құқылы. Мұндай жағдайда сұранысты орындау мерзімі Өнім беруші барлық қажетті әрі дұрыс ақпаратты алған сәттен бастап есептеледі.

15.3 Жауапкершілік:

Өнім беруші мыналар үшін жауапты болады:

• Тапсырыс берушінің Сұраныстарына сәйкес виртуалды желілік экранды (Firewall) әкімшілендіру бойынша осы талапта көзделген жұмыстардың орындалуына;

• Сұраныста көрсетілген параметрлер шегінде Firewall баптауларының дұрыс орындалуына;

• жұмыс уақытында Сұраныстарды өңдеу мен орындаудың белгіленген тәртібінің сақталуына;

• жұмыстарды орындау кезінде Firewall-дың штаттық функционалының пайдаланылуына.

Тапсырыс беруші мыналар үшін жауапты болады:

• Сұраныстарда көрсетілген ақпараттың дұрыстығына, толықтығына және қарама-қайшы еместігіне;

• Firewall баптауларының параметрлерін анықтауға және оларды қолдану бойынша қабылданатын шешімдерге;

• қажетті қолжетімділіктердің берілуіне және олардың дұрыс бапталуына;

• жұмыстарды орындау үшін қажетті ақпараттың уақтылы берілуіне.

Ерекше шарттар:

• Барлық жұмыстарды Өнім беруші Тапсырыс берушінің Сұраныстары негізінде орындайды;

• Өнім беруші Тапсырыс берушінің Сұранысында көрсетілген баптаулардың дұрыстығы мен мақсатқа сәйкестігіне талдау жүргізбейді;

• Өнім беруші Тапсырыс беруші қабылдаған архитектуралық шешімдер үшін жауапты болмайды;

• Сұранысты орындауға байланысты тәуекелдер анықталған жағдайда, Өнім беруші бұл туралы Тапсырыс берушіге хабарлауға құқылы, алайда жұмыстарды орындау туралы түпкілікті шешімді Тапсырыс беруші қабылдайды.

16. Резервтік көшіруді әкімшілендіруге қойылатын талаптар.

16.1 Резервтік көшірме жасауды әкімшілендіру қызметін Орындаушы Қызмет көрсетудің бүкіл мерзімі ішінде тұрақты негізде ұсынады және ол мыналарды қамтиды:

• Тапсырыс берушінің резервтік көшірме жасау жоспарына сәйкес резервтік көшірме жасау тапсырмаларын (Backup Job) баптауды, өзгертуді және сүйемелдеуді, соның ішінде қорғалатын объектілердің (ВМ, дискілердің, қосымшалардың) құрамын өзгертуді;

• кесте саясаттарын және сақтау мерзімі саясаттарын басқаруды, соның ішінде оларды Тапсырыс берушінің сұранысы бойынша түзетуді;

• резервтік көшірме жасау тапсырмаларының орындалуын күнделікті бақылауды, соның ішінде іркілістерге әрекет етуді және сәтсіз аяқталған тапсырмаларды қайта іске қосуды;

• осы техникалық ерекшеліктің 14-бөлімінде, 16.4-тармағында және №1 қосымшасында белгіленген тәртіппен және мерзімдерде Тапсырыс берушінің деректерді қалпына келтіруге (ВМ-ді толық қалпына келтіру, файлдарды/дискілерді ішінара қалпына келтіру) арналған өтінімдерін өңдеуді;

• резервтік көшірмелер қоймасының жай-күйін және қолжетімді көлемін бақылауды, соның ішінде бөлінген көлемнің пайдаланылуы шекті мәндерге жақындаған кезде Тапсырыс берушіге хабарлауды;

• резервтік көшірмелердің тұтастығы мен қалпына келтірілу мүмкіндігін мерзімді тексеруді (соның ішінде автоматты верификациялау құралдарымен);

• айына кемінде бір рет мерзімділікпен орындалған резервтік көшірме жасау тапсырмалары, инциденттер және қалпына келтіру мәртебесі туралы Тапсырыс берушіге есептілікті қалыптастыруды және ұсынуды;

• Тапсырыс берушімен келісілген технологиялық терезелерде резервтік көшірме жасау бағдарламалық жасақтамасының жаңартулары мен түзетулерін орнатуды.

16.2 Тапсырыс беруші сұранысты Өнім берушінің электрондық поштасына жібереді.

Виртуалды инфрақұрылым мен деректерді қалпына келтіруге арналған авариялық сұраныстарды Өнім беруші тәулік бойы (24/7/365) режимінде өңдейді және орындайды. Жоспарлы сұраныстар жұмыс уақытында: сағат 08:30-дан 18:00-ге дейін өңделеді.

16.3 Жұмыс уақытынан тыс уақытта түскен жоспарлы сұраныстар келесі жұмыс кезеңінде өңделуге және орындалуға тиіс.

16.4 Авариялық сұраныстарға әрекет ету мерзімі 15 минуттан, ал қалпына келтіру рәсімінің басталу уақыты олар тіркелген сәттен бастап 30 минуттан аспауға тиіс. Жоспарлы сұраныстарды орындау мерзімі 2 (екі) сағаттан 1 (бір) жұмыс күніне дейінгі уақытты құрайды

17. Шарттың Орындалу Деңгейін Есептеу (SLA)

17.1 Өзара есеп айырысу және SLA орындау сапасына жалпы бағалау жүргізу үшін Орындаушы «SLA орындау деңгейі» көрсеткішін есептейді.

17.2 Орындаушы Тапсырыс берушіге айына 99,9% қол жетімділік коэффициентімен қызметтер көрсетеді. Өзіне-өзі қызмет көрсету интерфейсі (%) - 98,0%

17.3 Тапсырыс берушімен келісілген жұмыстар жүргізілетін уақыт кезеңдері (жоспарлы регламенттік немесе авариялық) Қызметті үзу жағдайлары болып табылмайды. Жоспарлы техникалық жұмыстар туралы ақпарат Тапсырыс берушіге Орындаушы қызмет көрсеткен кезде № 2 кестеге - Үзілістер мен хабарламаларға сәйкес беріледі. Осы тармаққа сәйкес SLA есебінен шығарылатын барлық уақыт кезеңдерінің жалпы ұзақтығы (жоспарлы регламенттік, шұғыл және авариялық жұмыстар) жылына 36 сағаттан аспауы тиіс.

17.4 Орындаушы тек виртуалды инфрақұрылымның жұмысына жауап береді. Тапсырыс беруші пайдаланатын виртуалды инфрақұрылымның жұмысымен байланысты емес операциялық жүйелердің, ДҚБЖ немесе қолданбалы бағдарламалардың жұмысындағы кез келген іркілістер сервистің қолжетімділігі бойынша SLA есептеуге әсер етпейді. Бұл жағдайда әкімшілендіру және қалпына келтіру үшін жауапкершілік тек Тапсырыс берушінің құзыретіне ғана жүктеледі.

17.5 Жоспарлы регламенттік және шұғыл жұмыстар Тапсырыс берушіден жазбаша бекітуді алғаннан кейін ғана жүргізіледі. Тапсырыс беруші жұмыстарды жүргізу күнін/уақытын дәлелді түрде қабылдамауға және оларды Тапсырыс берушіге қандай да бір айыппұл санкцияларын қолданбай басқа күнге/уақытқа ауыстыруды ұсынуға құқылы.

17.6 Регламенттік жұмыстардың (қызмет көрсетудің) стандартты уақытынан тыс жүргізілетін жоспарлы техникалық жұмыстар туралы ақпарат жұмыс басталғанға дейін кемінде 48 сағат бұрын ұсынылады.

17.7 Регламенттік жұмыстардың (қызмет көрсетудің) стандартты уақытынан тыс жүргізілетін шұғыл жұмыстар туралы ақпарат жұмыс басталғанға дейін кемінде 12 сағат бұрын ұсынылады.

17.8 Жоспарлы техникалық және шұғыл жұмыстарды жүргізуді келісу үшін Орындаушы жүргізілетін жұмыстардың құрамын, уақытын, жауапты тұлғаны, қызметтерді көрсету кезіндегі жұмыстардың орындалуына жауапты тұлғаның

байланысын (жұмыс телефоны, ұялы телефоны, электрондық поштасы) және күтпеген жағдайларда қалпына келтіру жоспарын көрсете отырып, жұмыс жүргізу жоспарын жібереді.

17.9 Тараптар «Орындаушының Қызметтерді көрсетуі кезіндегі үзілістер мен хабарламалар» № 2 кестесінде көрсетілген Қызметтерге рұқсат беру үзілістерін штаттық режимде ұсыну ретінде саралауға және Қызметтерге қол жеткізбеу уақытында осындай үзілістерді, сондай-ақ салдары болып табылатын үзілістерді қамтымауға келіседі: - Тапсырыс берушінің Орындаушының келісімінсіз жүргізілетін, Орындаушының жауапкершілік аймағындағы Қызметтерге қол жеткізуге және/немесе аппараттық қамтамасыз етуге тікелей немесе жанама әсер ететін бағдарламалық қамтамасыз етудің баптауларын өзгертуі; - Тапсырыс беруші Орындаушымен Көрсетілетін қызметтерге қол жеткізу үшін қажетті шарттарды, оның ішінде ақы төлеу шарттарын қамтамасыз ету бөлігінде Шарттың талаптарын бұзған; - Тапсырыс беруші пайдаланатын бағдарламалық қамтамасыз етудің жұмысқа қабілетсіздігі немесе үйлеспеушілігі; - Тапсырыс берушінің кінәсінен болған Тапсырыс берушінің есептік деректеріне үшінші тұлғалардың қол жеткізуі; - Тапсырысшының ұсынылған есептеу ресурстарына (ГГц, Гб, IOPS) барынша рұқсат етілген жүктемеден асуы; - Шарттың талаптарына сәйкес айқындалған еңсерілмейтін күш жағдайлары.

17.10 Ұсынылатын АТ-сервистің нақты қолжетімділігі мынадай формула бойынша айқындалады: Сервистің нақты қолжетімділігі = (Т - Тавр)/Т * 100%, (немесе сервистің қолжетімділігі уақытының оны ұсынудың бағаланатын кезеңдегі келісілген уақытына қатынасы), мұндағы: Т - сервисті ұсынудың бағаланатын кезеңдегі келісілген уақыты; Тавр - сервистің келісілген уақыт ішінде қол жетімсіз болған нақты уақыты. Қызметтер көрсету кезінде Тапсырыс берушімен келісілген жұмыстар (жоспарлы регламенттік немесе шұғыл жұмыстар) жүргізілетін уақыт кезеңдері қызметтің қол жетімсіз жағдайлары болып табылмайды және № 2 кесте (Орындаушы қызметтер көрсету кезіндегі үзілістер мен хабарламалар) бойынша айқындалады. Сервистің АТ қолжетімсіздігі фактілері Тапсырыс берушінің АЖ жұмыс қабілеттілігін қалпына келтіру жөніндегі жұмыстар орындалғаннан кейін актіленеді. Сервистің АТ қолжетімсіздігінің басталу уақыты мынадай құжаттарға сүйене отырып есептеледі: жергілікті желі немесе сервистер, сондай-ақ Тапсырыс берушінің АЖ бойынша қолжетімсіздік оқиғалары көрсетілген мониторинг жүйесіндегі серверлердің/есептердің логтары (егер бұл VDC инфрақұрылымының істен шығуынан болған жағдайда); одан әрі логтарда немесе Проблемалық билетті ашуда расталған бірыңғай проблемасы бар Service-Desk ДБ-ға бірнеше жеке өтінімдер. Қол жетімділіктің аяқталу уақыты мыналарға сүйене отырып есептеледі: мониторинг (сервис) жүйесіндегі қалпына келтірілетін сервердің/есептердің логтары; жұмыс станцияларынан Тапсырыс берушінің сервисі мен АЖ қол жетімділік фактісі. Сервис қолжетімділігінің сәйкессіздігі үшін төлемақыны төмендету (айыппұл санкциялары) осы Техникалық ерекшелікке 3-қосымшаның № 3 кестесінде белгіленген өтемақы мөлшеріне сәйкес есептеледі.

18. Ақпаратты қорғау үшін жауапкершілікті бөлу

18.1 Жеткізуші тек өзінің іс-әрекеттерінен немесе әрекетсіздігінен туындаған салдарлар үшін ғана жауапты болады.

Тиісті оқиға тікелей Жеткізушінің осы Техникалық ерекшелікпен Жеткізушінің жауапкершілік және әкімшілендіру аймағына тікелей жатқызылған міндеттемелерді тиісінше орындамауынан туындаған жағдайда, Жеткізуші Тапсырыс берушінің ақпаратының жылыстауы (ағып кетуі), жоғалуы, бұрмалануы, бұғатталуы немесе оған рұқсатсыз қол жеткізілуі үшін жауапты болады.

Оқиғаның орын алу фактісінің өзі Жеткізушіге жауапкершілікті жүктеу үшін негіз болып табылмайды. Жауапкершілікті анықтау кезінде инциденттің туындау себебі, Тараптардың әрқайсысының жауапкершілік аймағы және тиісті Тараптың іс-әрекеттері немесе әрекетсіздігі мен туындаған салдарлар арасындағы тікелей себеп-салдарлы байланыстың болуы ескеріледі.

18.2 Жеткізуші жауапты емес:

1. тапсырыс берушінің, оның қызметкерлерінің, өкілдерінің, мердігерлердің не Тапсырыс беруші тарапынан ақпараттық ресурстарға қол жеткізген өзге де тұлғалардың әрекеттері немесе әрекетсіздігі;

2. тапсырыс берушінің есептік деректерін пайдалану, беру немесе компаға келтіру, сондай-ақ Тапсырыс берушінің тікелей кінәсінен орын алған Тапсырыс берушінің белгілі бір құқықтары мен қол жеткізу деңгейлері, егер Жеткізушінің қызметтерінің инфрақұрылымы мен сервистері деңгейінде осалдықтар, істен шығулар немесе рұқсатсыз қол жеткізу себеп болмаса;

3. тапсырыс берушінің қорғалатын және резервтелетін объектілердің құрамына қатысты шешімдері, резервтік көшірмелеу кестесі (оны Жеткізуші бойынша енгізуді қоспағанда), Тапсырыс берушінің резервтік көшірмелерді сақтау мерзімдерін, резервтелетін ақпараттың құрамы мен мазмұнын және өзге де параметрлерді айқындауы;

4. жеткізуші дұрыс орындаған жағдайда Firewall параметрлері, ережелері, саясаттары және жеткізуші белгілеген өзге де конфигурациялық шешімдермен;

5. архитектуралық шешімдер, конфигурациялар, операциялық жүйелер, мәліметтер базасы, қолданбалы бағдарламалық қамтамасыз ету және Әкімшілігі жеткізушінің жауапкершілік аймағына кірмейтін басқа компоненттер;

6. жабдықтаушының жауапкершілік аймағынан тыс орналасқан жабдық, байланыс арналары, бағдарламалық қамтамасыз ету және өзге де инфрақұрылым;

7. Жеткізуші өзінің жауапкершілік аймағы шегінде осы техникалық ерекшелікте көзделген қорғау, ден қою, жаңарту және хабарлама шараларын орындаған жағдайда, өндірушілердің және бұрын белгісіз осалдықтарды қоса алғанда, өзге де үшінші тұлғалардың бағдарламалық немесе аппараттық қамтамасыз етуінің осалдығы;

8. тапсырыс берушінің Жеткізуші ұсынған ақпараттық қауіпсіздіктің анықталған тәуекелдерін жою жөніндегі дәлелді жазбаша ұсынымдарды орындамауы немесе уақтылы орындамауы;

9. еңсерілмейтін күш мән-жайлары және Шартқа сәйкес жауапкершілік Жеткізушіге жүктелмейтін өзге де мән-жайлар.

18.3 Егер Жеткізуші тапсырма, жоспар, параметрлер немесе Тапсырыс берушінің сұрау салуы негізінде техникалық іс-қимылдарды орындаса, Жеткізуші берілген тапсырма шегінде тиісті техникалық іс-қимылдарды орындаудың дұрыстығына жауап береді.

Қосымша №1 Кесте №1 Инциденттің басымдығын анықтау

Қосымша №2 Кесте №2 - Орындаушы қызмет көрсету кезіндегі үзілістер мен хабарламалар

Қосымша №3 Кесте №3 - Қызметтің қолжетімділігі

Қосымша №4 - Сұрау Нысаны

**Қосымша**

| | |
|---|---|
| Приложение_№3_к_ТС_рус_каз.docx | |
| Приложение №4 к ТС рус каз.docx | |
| Приложение №2 к ТС рус каз.docx | |
| Приложение №1 к ТС рус каз.docx | |
| Қол қойған | Ергалиев Равиль Лукпанович |
| Қол қойылған күні | 23.11.2026 |

# ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

**по закупке 1267857 , Аренда облачных серверов**
**способом Открытый тендер**

**Лот № 1 (44 У, 4574282) Услуги по предоставлению вычислительных мощностей для физического размещения информации на сервере, постоянно находящемся в сети Интернет**

**Заказчик: Акционерное общество "Эмбамунайгаз"**

**Организатор: Акционерное общество "Эмбамунайгаз"**

## 1. Краткое описание ТРУ

| Наименование | Значение |
|---|---|
| Номер строки | 44 У |
| Наименование и краткая характеристика | Услуги по предоставлению вычислительных мощностей для физического размещения информации на сервере, постоянно находящемся в сети Интернет, Предоставление вычислительных мощностей для физического размещения информации на сервере, постоянно находящемся в сети Интернет (хостинг) |
| Дополнительная характеристика | Аренда облачных серверов |
| Количество | 1.000 |
| Единица измерения | - |
| Место поставки | КАЗАХСТАН, Атырауская область, Атырауская область, Г.АТЫРАУ, УЛ.ВАЛИХАНОВА 1 |
| Условия поставки | - |
| Срок поставки | с 01.2027 по 12.2029 (включительно) |
| Условия оплаты | Предоплата - 0%, Промежуточный платеж - 100%, Окончательный платеж - 0% |

## 2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

1. Определения и сокращения

ЦОД Центр обработки данных

Инфраструктура Поставщика Площадка, предназначенная для хранения, обработки и предоставления данных пользователям. Включающая в себя серверные комплексы, комплексы хранения данных, а также всю инженерную часть необходимую для функционирования и обеспечения безопасности ЦОД

СХД Система хранения данных

Ресурс Вычислительные ресурсы, дисковые пространства (SSD) для хранения данных

VDC Виртуальный дата центр, комплекс вычислительных ресурсов и систем для хранения данных объединённых в единую защищённую сеть под управлением ПО для виртуализации

VPN Виртуальная частная сеть

ИБ Информационная безопасность

ВМ Виртуальная машина (сервер)

ОС Операционная система

Рабочий день Означает день, официально считающийся в текущем году рабочим на территории Республики Казахстан при 5-дневной рабочей неделе

Инцидент Любое событие, выходящее за рамки стандартного функционирования ИТ-услуги и являющееся настоящей или возможной причиной приостановки или снижения качества предоставления этой услуги

Проблема Один или несколько связанных инцидентов с неизвестной причиной возникновения

Запрос на обслуживание Запрос на поддержку, предоставление информации, консультации или предоставление доступа в Гермозону

Время реакции Период времени между обращением к Исполнителю для получения технической поддержки и началом работы специалиста Исполнителя по решению возникшей проблемы Клиента

Время устранения Максимальное время, через которое обслуживаемая система восстановит работоспособность.

ДГУ Дизель–генераторная установка

Виртуальная машина Программная рабочая станция, которая по аналогии с физической рабочей станцией может запускать операционные системы и приложения

vApp Контейнер, в котором размещаются виртуальные машины, который позволяет объединять виртуальные машины по их назначению (почтовый сервер, бухгалтерия и пр.) и управлять группой виртуальных машин

ИС Информационная Система

ИТ Информационные технологии

Проблемный билет Заявка, открытая в системе Service-Desk по нескольким однородным проблемам

Внештатное отключение Все случаи отключения без предварительного уведомления со стороны Заказчика

Аварийный случай Внештатное отключение виртуальной машины, vApp, VDC, вызванные сбоем инфраструктуры VDC

Интерфейс самообслуживания Это веб-портал (панель управления), предоставляемый Заказчику для самостоятельного управления выделенными облачными ресурсами (виртуальными машинами, сетями, хранилищами). Интерфейс предназначен для выполнения административных и сервисных операций, мониторинга использования ресурсов и получения информации о состоянии сервисов. Работоспособность интерфейса самообслуживания не влияет на доступность предоставляемых вычислительных и сетевых ресурсов

СРК Система резервного копирования

Firewall Виртуальный межсетевой экран (Firewall)

2. Цель

Настоящий объем услуги определяет состав, характеристики и требования к услуге аренды виртуальных вычислительных ресурсов, предоставляемых в формате изолированной облачной среды с удалённым доступом (далее — Услуга предоставления вычислительных мощностей).

Услуга предоставляется под размещение следующих информационных систем Заказчика:

1) SAP S/4HANA;

2) Горизонтальный мониторинг;

3) Архивное хранение данных.

Цель оказания Услуги — обеспечение отказоустойчивой, гибкой и масштабируемой ИТ-инфраструктуры согласно указанному объему услуг и техническим характеристикам.

Настоящий объем услуг устанавливает технические, функциональные и эксплуатационные требования к вычислительным ресурсам, системе хранения, сетевой инфраструктуре, информационной безопасности и качеству обслуживание.

3. Общие требования

3.1 Место оказания услуги — Республика Казахстан, г. Атырау

3.2 Услуга представляет собой совокупность виртуальных вычислительных ресурсов (серверы, диски и сети), доступных через изолированные каналы связи, и ряд дополнительных услуг, таких как резервное копирование, управление, техническое обслуживание

3.3 Услуга предоставляется с целью обеспечения непрерывности предоставления ИТ услуг Заказчика, увеличение гибкости и масштабируемости ИТ инфраструктуры

3.4 Услуга включает полную миграцию всех информационных систем Заказчика, из текущей инфраструктуры Заказчика в инфраструктуру Поставщика. Миграция выполняется силами и за счёт Поставщика и завершается не позднее 5 (пяти) календарных дней с даты предоставления Заказчиком доступа к исходной инфраструктуре. Миграция выполняется без остановки работы ИС Заказчика. Миграция считается завершённой с даты подписания сторонами акта, который подписывается после подтверждения работоспособности всех ИС в инфраструктуре Поставщика.

4. Требования к ЦОД

4.1 ЦОД представляет собой отдельно стоящее капитальное сооружение (здание) (далее - ЦОД). Здание спроектировано и построено для размещения машинного зала, обеспечивающего функционирование высокотехнологичного оборудования для обработки и хранения данных. Объект находится на выделенном земельном участке, что гарантирует независимость и безопасность эксплуатации

4.2 ЦОД должен находиться на охраняемой территории с круглосуточной физической охраной. Въезд на территорию должен осуществляться через ворота, оборудованные противотаранными устройствами. Дата-центр должен быть спроектирован и построен в соответствии с требованиями уровня TIER III

4.3 Для возможности обслуживания инфраструктуры Заказчика без отключения инженерной инфраструктуры ЦОД должен быть оснащен резервными компонентами.

4.4 ЦОД должен иметь два независимых ввода электропитания от двух различных трансформаторных подстанций, обеспечивающих полное резервирование питания по схеме 2N с автоматическим вводом резерва (АВР) и физически раздельными кабельными трассами. К надежности электроснабжения предъявляются следующие требования: - в случае потери энергоснабжения, серверное и сетевое оборудование должно автоматически перейти на резервное энергоснабжение (ДГУ) Исполнителя. При переходе на резервный источник энергоснабжения непрерывность предоставляемого сервиса не должна быть нарушена

4.5 Для обеспечения работы ИТ-нагрузки в любой отдельно взятый момент времени достаточно работы одного канала распределения, как входного участка системы энергоснабжения, так и для механических систем

4.6 Постоянной установленной мощности активных компонентов должно быть достаточно для обеспечения всех потребностей оборудования ЦОД, когда резервные компоненты и каналы распределения по той или иной причине выведены из эксплуатации

4.7 ЦОД должен быть оснащен современной автоматической системой газового пожаротушения, современной климатехникой и безотказной системой гарантированного питания электрической сети (наличие источников бесперебойного питания и дизельной электростанции)

4.8 ЦОД должен иметь на территории центр мониторинга инженерных систем и дежурных специалистов технической поддержки для сокращения времени реакции на запросы и события

4.9 ЦОД должен находиться под круглосуточной охраной лицензированного охранного агентства, обеспечивающего физическую защиту объекта в режиме 24/7

4.10 На объекте должна быть реализована многоуровневая система охраны периметра, включающая: Видеонаблюдение по периметру и внутри здания с архивом хранения не менее 90 (девяносто) календарных дней; Датчики движения и проникновения на периметре; Тревожные кнопки на постах охраны

4.11 ЦОД должен иметь офисные или рабочие помещения, доступные для размещения сотрудников Заказчика, по запросу

4.12 ЦОД должен быть оборудован отдельной зоной приёма и разгрузки оборудования с подъездом для тяжёлого транспорта и тележками для перемещения по зданию.

4.13 Должна быть предусмотрена зона временного хранения оборудования Заказчика (не менее 10 кв.м), с охраной и контролем доступа

4.14 ЦОД должен иметь отдельное складское помещение, предназначенное для хранения оборудования, материалов и иных активов Заказчика

4.15 ЦОД должен иметь отдельное помещение (зону) для предварительной проверки и настройки оборудования Заказчика до его ввода в эксплуатацию

4.16 Поставщик обязан обеспечить возможность размещения ИТ-инфраструктуры Заказчика в геораспределённой архитектуре, предусматривающей размещение не менее чем в трёх физически независимых центрах обработки данных (ЦОД), включающих основной и 2 резервные ЦОД, физически удалённых друг от друга на безопасное расстояние в соответствии с требованиями пункта 153 Единых требований в области информационнокоммуникационных технологий и обеспечения информационной безопасности, утверждённых постановлением Правительства Республики Казахстан от 20.12.2016 № 832, и обеспечивающих отказоустойчивость и катастрофоустойчивость информационных систем Заказчика. Поставщик обязан предоставить подтверждение права владения или наличия в аренде не менее трех отдельно стоящих зданий ЦОД, в течение двух рабочих дней с момента подписания договора

5. Требования к каналам связи

5.1 Требования по каналам связи предоставляемым Поставщиком Заказчику в рамках оказания Услуги: Поставщик должен организовать два независимых канала связи L2, основной - 500 мбит/с и резервный - 200 мбит/с. от ЦОД поставщика до адреса заказчика. Адрес заказчика: Ул. Шокана Валиханова 1, г. Атырау

6. Требования к ресурсам

6.1 Вычислительные ресурсы предоставляются согласно техническим требованиям указанные в данном объеме услуг

6.2 Поставщик должен обеспечить Заказчику централизованное управление арендуемыми ресурсами

6.3 Заказчик имеет право запросить дополнительные мощности (процессорные, дисковое пространство, оперативная память) при наличии технической возможности со стороны Поставщика на услугу путем направления заявки в

электронном виде посредством электронной почты, время на предоставление дополнительных мощностей после заявки не должно превышать 2 (два) рабочих дня при наличии технической возможности у Поставщика, до 60 рабочих дней – при ее отсутствии

6.4 При использовании вычислительных ресурсов Заказчик имеет право отказаться от части мощностей (процессорных, дискового пространства, оперативной памяти) путём направления Заявки на уменьшение на официальный адрес Поставщика с корпоративного домена Заказчика, указанного в Договоре. Заявка должна содержать: (i) перечень ресурсов и величину уменьшения по каждому типу; (ii) желаемую дату вступления изменений в силу; (iii) подтверждение уплаты всех начислений за прошедшие периоды. Уменьшение объёма вступает в силу с момента подписания дополнительного соглашения сторонами

6.5 В случае полного отказа Заказчиком от использования вычислительных ресурсов, Исполнитель в течение 14 календарных дней архивирует все данные, находящиеся на ресурсах Исполнителя, и предоставляет Заказчику возможность их скачивания по защищённому каналу или копирования на собственные съёмные носители. Исполнитель обязуется в течение 30 календарных дней не удалять со своих ресурсов данные Заказчика. При этом Заказчик оплачивает стоимость услуг Исполнителя в течение срока хранения информации Заказчика на ресурсах Исполнителя. Дальнейшее хранение данных возможно по согласованным тарифам Исполнителя

6.6 Вычислительные ресурсы предоставляются по действующим тарифам Поставщика. Факт предоставления дополнительных мощностей фиксируется Дополнительным соглашением к Договору, которое должно быть заключено в течение 30 (тридцати) дней с момента начала использования ресурсов

7. Требования к функционалу

7.1 Возможность «горячего» расширения текущих дисков ВМ, и добавления новых дисков

7.2 Возможность создания снимков состояния виртуальных машин (как работающих, так и остановленных), в рамках арендуемых ресурсов

7.3 Создание и удаление виртуальных машин (ВМ) с указанием необходимых параметров (vCPU, RAM, NVMe, ОС и др.); Включение, выключение, перезагрузка и приостановка ВМ через интерфейс; Изменение конфигурации ВМ: изменение числа виртуальных процессоров (vCPU); изменение объема оперативной памяти (RAM); добавление, удаление и изменение виртуальных дисков; изменение сетевых адаптеров и их привязка к виртуальным сетям; Выбор и установка операционных систем и приложений на основе предоставленных шаблонов (VM templates / vApp templates) либо ISO-образов; Импорт собственных ISO-образов и шаблонов ВМ в виртуальную организацию; Изоляцию сетевого пространства Заказчика от других пользователей системы (tenant isolation); Самостоятельное создание и удаление виртуальных сетей (Org VDC networks); Настройку фаерволов, NAT, маршрутов и VPN на уровне виртуального маршрутизатора

7.4 Требования к СРК: Система должна обеспечивать резервное копирование виртуальных машин, с поддержкой инкрементального копирования с использованием технологии отслеживания изменённых блоков.

Необходимо обеспечить централизованное управление заданиями резервного копирования, восстановления и репликации, с возможностью создания политик по расписанию и политики срока хранения.

Система должна поддерживать автоматическую проверку резервных копий на предмет целостности и возможности восстановления.

Хранилище резервных копий должно поддерживать дедупликацию, сжатие, а также защиту от удаления (immutable backup) на уровне настроек хранилища. Резервные копии всех критически важных данных должны выполняться на выделенную систему хранения данных (СХД), физически отделённую от основной СХД, используемой для продуктивных данных. Размещение резервных копий на той же СХД, что и основные данные, не допускается. Исполнитель обеспечивает возможность резервного копирования баз данных, систем и виртуальных машин на ленточные библиотеки или дисковые массивы. Услуги, описанные в данном пункте, включая предоставление ПО для резервного копирования, выполнение операций резервного копирования по согласованному расписанию и хранению данных в объеме, указанном в пункте 13,1 входят в стоимость услуг по Договору

7.5 Исполнитель обеспечивает каталог образов популярных операционных систем. В случае отсутствия необходимого образа операционной системы или версии системы операционной системы, Заказчик информирует Исполнителя о необходимости загрузки дополнительных образов

7.6 Исполнитель вправе запросить образ у Заказчика для последующей публикации в каталоге

7.7 Исполнитель вправе отказать в размещении образа в каталоге, в случаях если данный образ нарушает Законодательство РК и/или содержит потенциальную угрозу для безопасности ИТ инфраструктуре (в том числе ПО для майнинга, взлома или устаревшие продукты с законченным циклом поддержки со стороны производителя или сообщества)

7.8 Допускается после согласования с Заказчиком использование альтернативных гипервизоров.

7.9 Поддержка 32- и 64-битных гостевых ОС, работающих на серверах стандартной архитектуры x86

8. Требования к физической и информационной безопасности

8.1 Поставщик обеспечивает конфиденциальность, целостность и доступность для Заказчика всех его данных, размещенных в ЦОД

8.2 Поставщик обеспечивает возможность переноса (миграции) резервных копий, образов виртуальных машин и данных Заказчика в рамках Услуги в другой ЦОД (по требованию Заказчика). Перенос (миграция) осуществляется Заказчиком самостоятельно в рамках данной Услуги без увеличения стоимости Договора. После подтверждения Заказчиком полной миграции образов виртуальных машин и данных, Поставщик обязуется уничтожить все данные Заказчика, предоставив документальные доказательства факта уничтожения

8.3 Поставщик обязуется гарантировать изоляцию виртуальных ресурсов в пределах, выделенных Заказчику

8.4 Поставщик обеспечивает ограничение физического доступа посторонних лиц к оборудованию ЦОД

9. Требования к технической поддержке

9.1 Круглосуточная гарантированная техническая поддержка Услуги будет всегда доступна для регистрации и обработки заявок Заказчика в течение всего срока оказания Услуги через единую службу технической поддержки посредством телефонных звонков (телефонная линия будет всегда доступна для входящих звонков Заказчика) и электронной почты

9.2 Поставщик предоставит контактные данные службы технической поддержки для регистрации обращений, с указанием ответственных лиц (технических специалистов)

9.3 Служба технической поддержки Поставщика будет функционировать в непрерывном режиме: «24 (двадцать четыре) часа в сутки, 7 (семь) дней в неделю» включая выходные и праздничные дни, в течение всего срока оказания Услуги

9.4 В случае обнаружения Заказчиком Инцидента и аварийных ситуации в работе Услуги, Заказчик информирует службу технической поддержки о наличии Инцидента. Информация об Инциденте предоставляется по телефону(-ам) или электронным сообщением по электронной почте, либо другим иным способом, по согласованию с Заказчиком

9.5 Работы, требующие временного отключения услуги на стороне Поставщика, должны проводиться в нерабочее время или выходные и праздничные дни. Поставщик должен уведомить официальным письмом заказчика не менее чем за 3 (три) рабочих дня и и получить письменное согласие от Заказчика до начала проведения работ

9.6 Время реагирования на запрос Заказчика по выявленной проблеме не должно превышать 15 минут в рабочее время и 45 мин в не рабочее время, устранение массовых повреждений не должно превышать 2 (двух) часов. Поставщик сообщает Заказчику номер зарегистрированного Инцидента, время регистрации Инцидента с кратким описанием Инцидента

9.7 Поставщик обязуется обеспечить журналирование всех событий инфраструктуры (виртуальной, сетевой и т. д.) и предоставить доступ к журналам событий по официальному запросу Заказчика

9.8 В случае аварийных ситуаций или перерывов в оказании Услуг Авторизованный пользователь регистрирует инцидент в Службе сопровождения Заказчиков. Простой отсчитывается с момента регистрации инцидента до уведомления о возобновлении Услуги. Под аварийной ситуацией понимается аварийное завершение процесса, выполняемого той или

иной подсистемой, связанное с прерыванием предоставления услуги, предусмотренной договором. При работе системы возможны следующие аварийные ситуации, которые влияют на надежность работы системы: -сбой в электроснабжении серверного и сетевого оборудования, на базе которого построена площадка VDC; - сбой в электроснабжении инфраструктуры Гермозоны; - сбои в работе программно-аппаратного комплекса площадки VDC. В случаях, когда сбой привел к отсутствию работоспособности система заказчика, время недоступности рассчитывается с момента регистрации инцидента

9.9 Цикл обработки запросов, проблем, заявок должен быть построен таким образом, чтобы все запросы были зафиксированы и ни одна проблема не осталась неразрешенной. Заказчику сообщается об изменении статуса обработки обращения и статуса проблемы

9.10 Отказ одного оборудования (сервера, сетевого оборудования, оборудования безопасности) не должно приводить к остановке сервиса; Инфраструктура Поставщика должна быть отказоустойчивой и надежной для предоставления качественной и бесперебойной услуги

9.11 Поставщик должен обеспечить коэффициент отказоустойчивости ЦОД не менее 99,9%

9.12 Поставщик обязан иметь оперативную службу технической поддержки на круглосуточной основе, которая будет принимать заявки, поступающие от Заказчика на предмет устранения повреждений и т. д., посредством электронной почты, телефонной связи, и рассылать уведомления, касающиеся Заказчика, посредством электронной почты, телефонной связи

9.13 Поставщик в течение 2 (двух) рабочих дней с даты заключения Договора должен подтвердить наличие и доступность ресурсов, согласно объему, указанного в настоящей технической спецификации для размещения ИС Заказчика

9.14 Поставщик в течение 2 (двух) рабочих дней с даты заключения Договора должен предоставить письмо о наличии основного ЦОД и 2 резервных ЦОД с указанием адреса расположения

9.15 Режим функционирования услуги должен поддерживаться 24 часа 7 дней в неделю.

9.16 Исполнитель гарантирует работоспособность и время восстановления VDC в случае аварийных ситуаций

9.17 Так же по запросу Заказчика Исполнитель может разработать и предоставить план восстановления в резервном ЦОД

9.18 Процессы службы технической поддержки Исполнителя должны поддерживаться соответствующей системе Service desk

9.19 В случае массовых повреждениях инфраструктуры Поставщика срок устранения может быть продлен не более чем на 2 (два) часа исключительно по мотивированному согласованию с Заказчиком, с предоставлением почасового отчета о ходе аварийно-восстановительных работ

9.20 Массовые повреждения это несколько единичных заявок в БД Service Desk с единой проблемой, подтверждённой далее в логах или открытием Проблемного билета

9.21 Заказчик должен иметь возможность средствами тенанта заказчика видеть потребляемые ресурсы, выделенные ему

9.22 Исполнитель обязуется по запросу Заказчика провести детальную демонстрацию используемого оборудования на уровне виртуализации и в ЦОД

9.23 При возникновении комплексных инцидентов Поставщик инфраструктуры обязан по запросу Заказчика обеспечивать участие дежурного инженера в совместных рабочих группах с привлечением другого подрядчика Заказчика по сопровождению прикладного ПО, а также предоставлять логи платформы виртуализации, СХД и сети задействованных в оказаниях Услуги по запросу Заказчика в течение не более 2 часов с момента запроса

10. Технические требования к серверному оборудованию, системе хранения данных и сетевому оборудованию

10.1 Серверное оборудование: Серверное оборудование должно отвечать следующим требованиям. Архитектура: не менее двух сокетов на базе современных серверных процессоров x86-64. Процессоры: не ниже уровня серверных процессоров 4-го поколения, не менее 32 физических ядер на каждый процессор, с тактовой частотой не ниже 2,8 ГГц. Память: поддержка оперативной памяти не менее DDR5 с эффективной частотой не ниже 5600 MT/s, возможность установки модулей с функцией коррекции ошибок (ECC). Общий объём установленной оперативной памяти на сервер — не менее 2000 ГБ, с возможностью дальнейшего расширения. Сетевые интерфейсы: наличие не менее двух адаптеров, каждый с двумя портами скоростью не ниже 25 Гбит/с, поддерживающих технологии виртуализации ввода-вывода (SR-IOV, VLAN, VXLAN). Поддержка аппаратного мониторинга, удалённого управления и out-of-band-доступа (например, IPMI или аналог). Серверное оборудование должно быть сертифицировано для работы с ПО SAP HANA (Tailored Data Center Integration или Certified Solution). Сертификация оборудования (Tailored Data Center Integration или Certified Solution) должна быть опубликована на портале поддержки SAP

10.2 Система хранения данных (СХД): Используемая система хранения данных должна иметь: Полное резервирование контроллеров (HA-конфигурация); Пропускная способность каждого порта не менее 25 Гб/с (гигабит в секунду); Поддержку RAID DP или эквивалентной технологии, обеспечивающей отказоустойчивость при выходе из строя не менее двух дисков, наличие Spare Disk; Технологии эффективного использования дискового пространства, включая дедупликацию, компрессию и thin provisioning; NVMe SSD-диски, оптимизированные под высоконагруженные IOPS-сценарии; Поддержку протоколов iSCSI, NFS, S3 и SMB. Система хранения данных должна быть сертифицирована для работы с ПО SAP HANA (Tailored Data Center Integration или Certified Solution). Сертификация оборудования должна быть опубликована на портале поддержки SAP

10.3 Система хранения данных под резервное копирования: Используемая система хранения данных должна иметь: Полное резервирование контроллеров (HA-конфигурация); Пропускная способность каждого порта не менее 25 Гб/с (гигабит в секунду); Поддержку RAID DP или эквивалентной технологии, обеспечивающей отказоустойчивость при выходе из строя не менее двух дисков; NL диски; Поддержку протоколов iSCSI

10.4 Сетевое оборудование: Коммутационное оборудование должно обеспечивать: Наличие не менее 48 портов 25GbE (SFP28) с поддержкой агрегации (LACP); Наличие портов 100GbE (QSFP28) в количестве не менее 8; Наличие резервирования по питанию и вентиляции; Совместимость с протоколами RoCEv2, LLDP, LACP, BGP, EVPN и VXLAN; Поддержку сегментации трафика и VLAN для обеспечения ИБ и многопользовательского разделения; Должен поддерживаться транзакционный подход применения конфигурации, чтобы в случае ошибки при настройке функционала можно было произвести откат; Поддержка механизма автоматического отката транзакции применения конфигурации, в случае ручного неподтверждения

11. Требование к сертифицированной ОС совместимой с подсистемой SAP

11.1 Общие требования: Операционная система: корпоративный Linux-дистрибутив с длительной поддержкой и проверенной совместимостью с SAP; Ядро Linux версии не ниже 4.12, рекомендуется версия 4.18 и выше; Менеджер пакетов: поддержка RPM-пакетов с системой разрешения зависимостей; Основная файловая система: EXT3, EXT4, XFS или Btrfs; Настройки для оптимальной работы SAP с файловыми системами (например, использование опции монтирования noatime для рабочих каталогов SAP); Размеры разделов должны соответствовать требованиям SAP, включая выделенное пространство для логов, временных файлов и резервных копий; Настройка параметров ядра для улучшения работы SAP; Мониторинг производительности с использованием стандартных Linux-инструментов и специализированных SAP утилит; Иметь официальную техническую поддержку на срок действия договора; Включать регулярные обновления безопасности и исправлений

12. Требования к виртуальному межсетевому экрану (firewall)

12.1 Общие требования: Лицензирование на неограниченное количество пользователей. В состав поставляемой лицензии должна входить официальная прямая техническая поддержка от производителя виртуального межсетевого экрана (firewall) в режиме 24/7 на весь период оказания Услуги предоставления вычислительных мощностей. Поддержка должна включать:

- Доступ к обновлениям, консультациям и регистрации обращений.

- Регулярное автоматическое обновление сигнатур модулей безопасности и перечней угроз.

Виртуальный межсетевой экран (firewall) должен иметь возможность установки и сопровождения на ведущих платформах виртуализации: VMware ESXi, Microsoft Hyper-V, KVM, Xen

12.2 Функциональные возможности: Поддержка межсетевого экранирования с фильтрацией по IP, портам, приложениям. Управление полосой пропускания (Traffic Shaping) и балансировка нагрузки. Поддержка NAT, PAT, маршрутизации на основе политик, VLAN tagging (802.1Q). Встроенная поддержка VPN (PPTP, IPSec, SSL), включая топологии hub-and-spoke, и аутентификацию по сертификатам IKE. Автоматическое обновление сигнатур и возможность настройки пользовательских правил. Инспекция SSL-трафика с интеграцией через ICAP-протокол. Контроль приложений, защита от DoS, фильтрация по URL, категориям сайтов и MIME-заголовкам. Функции антивирусной защиты, антиспам-фильтрации, DLP (предотвращение утечек данных). Поддержка SD-WAN и оптимизации WAN-соединений. Возможность управления через Web-интерфейс и CLI, поддержка журналирования и интеграции с SIEM-системами

12.3 Поддержка пользователей и аутентификация: Аутентификация через внутреннюю базу, Active Directory, RADIUS /LDAP, IP/MAC, групповые политики. Многоуровневая модель администрирования с разграничением ролей

12.4 Ресурсные параметры: Поддержка разделения одного виртуального межсетевого экрана на не менее 10 (десяти) логических независимых виртуальных устройств с раздельной маршрутизацией и независимыми политиками безопасности, не менее 10 (десяти) виртуальных сетевых интерфейсов, не менее 2 (двух) ядер (vCPU), не менее 2 (двух) ГБ виртуальной оперативной памяти (vRAM) и 32 (тридцать два) ГБ локального хранилища. Поддержка не менее 10 000 (десяти тысяч) правил фильтрации трафика. Пропускная способность при включенном комплексе базовых проверок безопасности (IPS и инспекция SSL/TLS): не менее 500 Мбит/с (в соответствии с пропускной способностью интернет-канала заказчика)

12.5 Подписка на сервисы: Наличие активной подписки на ключевые сервисы: IPS, антивирус, антиспам, фильтрация web-контента, облачная песочница (cloud sandbox)

13. Требования к предоставляемому объему вычислительных ресурсов

Виртуальный процессор vCPU указан из расчета частоты один ГГц на один vCPU. При создании виртуальной машины должна быть возможность выделения не менее 64 vCPU и не менее 200 ГБ оперативной памяти.

13.1. Сводный объем по Договору

| № | Продукт | Ед. изм. | Кол-во |
|---|---|---|---|
| 1 | Виртуальный процессор vCPU | Ghz | 1 792 |
| 2 | Виртуальная оперативная память vRAM | GB | 5 316 |
| 3 | Предоставление дискового пространства SSD NVMe | GB | 111 598 |
| 4 | Предоставление дискового пространства со скоростью не менее 10K или эквивалентной технологии | GB | 117 256 |
| 5 | Система резервного копирования | VM | 72 |
| 6 | Виртуальный межсетевой экран (Firewall) | Лицензии | 1 |
| 7 | ОС для серверов SAP | Лицензии | 14 |
| 8 | ОС для серверов общего назначения | Лицензии | 15 |
| 9 | Администрирование резервного копирования | Месяц | 36 |
| 10 | Администрирование виртуального межсетевого экрана (Firewall) | Месяц | 36 |

11 Предоставление в аренду канала связи L2VPN (Основной) Мбит/с 500

12 Предоставление в аренду канала связи L2VPN (Резервный) Мбит/с 200

14. Требования к резервному копированию и аварийному восстановлению

14.1 • Поставщик обеспечивает резервное копирование и восстановление на инфраструктурном уровне: виртуальных машин (ВМ), виртуальных дисков (NVMe/SSD), конфигураций vApp, настроек виртуальных сетей и правил Firewall.

• Поставщик предоставляет и обслуживает платформинг системы резервного копирования (СРК) — ПО, агенты виртуализации, выделенную СХД под бэкапы и изолированные каналы передачи данных.

• Поставщик обеспечивает техническую возможность выполнения консистентных снимков (Application-Consistent Snapshots) и предоставляет интерфейсы/инструменты СРК для взаимодействия с Заказчиком и/или третьими лицами, администрирующими прикладное ПО и СУБД.

• Резервное копирование осуществляется в соответствии согласованным Заказчиком планом Резервного копирования. Объем резервного копирование не должен превышать Пункта 13.1. Технической спецификации.

14.2 Инфраструктурные метрики непрерывности (RPO и RTO)

Поставщик гарантирует соблюдение следующих показателей на уровне платформы виртуализации и СХД:

• Для продуктивной инфраструктуры (ВМ под SAP S/4HANA и Горизонтальный мониторинг):

o Инфраструктурный RPO (Recovery Point Objective): не более 24 часов для полных образом ВМ;

o Инфраструктурный RTO (Recovery Time Objective): согласовывается в план-графике резервного копирования.

• Для некритичных и архивных ВМ:

o RPO: не более 24 часов;

o RTO: согласовывается в план-графике резервного копирования.

• Поставщик обязуется организовать резервное копирование виртуальных машин в соответствии с планом резервного копирования Заказчика, в рамках выделенного объема дискового пространства для резервного копирования. Возможность полного, инкрементального резервного копирования.

14.3 Администрирование и защита данных СРК

• Поставщик организует и круглосуточно сопровождает процессы резервного копирования ВМ в соответствии с утвержденным с Заказчиком расписанием.

• Резервные копии размещаются на отдельной СХД, физически и логически изолированной от продуктивных дисковых массивов.

• Поставщик обеспечивает защиту хранилища резервных копий от несанкционированного удаления, перезаписи и шифрования (технология Immutable Backup / WORM) на уровне настроек СХД.

14.4 Контрольные восстановления и верификация (Sandbox Testing)

• Поставщик обеспечивает ежедневный автоматический контроль целостности контрольных сумм резервных копий.

• Поставщик обязан ежемесячно проводить тестовое контрольное разворачивание случайным образом выбранных ВМ /дисков Заказчика в изолированный тестовый сегмент (Sandbox) с проверкой успешности загрузки операционной системы и доступности виртуальных дисков.

• Результаты проведенных верификаций и тестовых восстановлений фиксируются в Ежемесячном отчете СРК, предоставляемом Заказчику.

14.5 Мониторинг и техническое взаимодействие

• Поставщик осуществляет круглосуточный мониторинг (24/7) состояния заданий СРК. В случае сбоя Поставщик обязателен в течение 2 (двух) часов устранить инфраструктурнLую причину сбоя и перезапустить копирование.

• При проведении работ по восстановлению систем Поставщик выделяет дежурного инженера для оперативно-технического взаимодействия со специалистами Заказчика и подрядчиками по прикладным ИС.

15. Требования к администрированию Firewall

15.1 Общие требования: Поставщик по запросу Заказчика осуществляет техническое содействие по администрированию администрированию виртуального межсетевого экрана (Firewall) (далее – Firewall).

Содействие в администрировании Firewall выполняется через организованное Заказчиком VPN-соединение либо через панель VDC с ограниченным доступом только до Firewall. Заказчик создает и передает Поставщику учетную запись для подключения к Firewall.

В рамках оказания технического содействия Поставщик по запросу Заказчика выполняет:

- создание, изменение, удаление сетевых интерфейсов на Firewall;

- создание, изменение, удаление политик Firewall на основании запроса Заказчика по форме приложения №4 (далее – Запроса);

- обновление Firewall;

- резервное копирование конфигурации Firewall.

15.2 Порядок отправки и выполнения запроса: Заказчик направляет запрос на электронную почту Поставщика. Поставщик выполняет обработку и исполнение запросов в рабочее время: с 08:30 до 18:00. Аварийные запросы, связанные с блокировкой критического трафика на Firewall, обрабатываются и исполняются в круглосуточном режиме (24/7/365) в сроки, установленные для Высокого приоритета (Приложение №1). При необходимости проведения перезагрузки или обновления Firewall время выполнения работ подлежит предварительному согласованию с Заказчиком, но в интервале рабочего времени Поставщика (за исключением аварийных ситуаций, требующих экстренной перезагрузки для восстановления доступности ИС).

Плановые запросы, поступившие в нерабочее время, подлежат обработке и исполнению в следующий рабочий период.

Срок обработки и выполнения запросов определяется Поставщиком в зависимости от сложности и составляет от 2 (двух) часов до 1 (одного) рабочего дня.

В случае предоставления Заказчиком неполной или некорректной информации Поставщик вправе запросить дополнительные сведения. В таком случае срок выполнения запроса исчисляется с момента получения Поставщиком всей необходимой и корректной информации.

15.3 Ответственность:

Поставщик несет ответственность:

- за выполнение работ, предусмотренных настоящим требованием к администрированию виртуального межсетевого экрана (Firewall), в соответствии с Запросами Заказчика;

- за корректность выполнения настроек Firewall в пределах параметров, указанных в Запросе;

- за соблюдение установленного порядка обработки и выполнения Запроса в рабочее время;

- за использование штатного функционала Firewall при выполнении работ.

Заказчик несет ответственность:

- за корректность, полноту и непротиворечивость информации, указанной в Запросах;

- за определение параметров настроек Firewall и принимаемые решения по их применению;

- за предоставление необходимых доступов и их корректную настройку;

- за своевременное предоставление информации, необходимой для выполнения работ.

Особые условия:

- Все работы выполняются Поставщиком на основании Запросов Заказчика;

- Поставщик не осуществляет анализ корректности и целесообразности настроек, указанных в Запросе Заказчика;

- Поставщик не несет ответственности за архитектурные решения, принятые Заказчиком;

- В случае выявления рисков, связанных с выполнением Запроса, Поставщик вправе уведомить Заказчика, однако окончательное решение о выполнении работ принимает Заказчик.

16. Требования к администрированию резервного копирования.

16.1 Услуга администрирования резервного копирования предоставляется Исполнителем на постоянной основе в течение всего срока оказания Услуги и включает:

- настройку, изменение и сопровождение заданий резервного копирования (Backup Job) в соответствии с планом резервного копирования Заказчика, включая изменение состава защищаемых объектов (ВМ, дисков, приложений);

- управление политиками расписания и политики срока хранения, включая их корректировку по запросу Заказчика;

- ежедневный контроль выполнения заданий резервного копирования, включая реагирование на сбои и повторный запуск неуспешных заданий;

- обработку заявок Заказчика на восстановление данных (полное восстановление ВМ, выборочное восстановление файлов/дисков) в порядке и в сроки, определённые разделом 14, пунктом 16.4 и приложением №1 настоящей технической спецификации;

- контроль состояния и доступного объёма хранилища резервных копий, включая уведомление Заказчика при приближении к предельным значениям использования выделенного объёма;

- проведение периодических проверок целостности и восстанавливаемости резервных копий (в том числе средствами автоматической верификации);

- формирование и предоставление Заказчику отчётности о выполненных заданиях резервного копирования, инцидентах и статусе восстановления с периодичностью не реже одного раза в месяц;

- установку обновлений и исправлений программного обеспечения резервного копирования в согласованные с Заказчиком технологические окна.

16.2 Заказчик направляет запрос на электронную почту Поставщика.

Аварийные запросы на восстановление виртуальной инфраструктуры и данных обрабатываются и исполняются поставщиком в непрерывном круглосуточном режиме (24/7/365). Плановые запросы обрабатываются в рабочее время с 8.30 до 18.00

16.3 Плановые запросы, поступившие в нерабочее время, подлежат обработке и исполнению в следующий рабочий период.

16.4 Срок реакции на аварийные запросы составляет не более 15 минут, время начала процедуры восстановления – не более 30 минут с момента регистрации. Срок выполнения плановых запросов составляет от 2(двух) часов до 1(одного) рабочего дня.

17. Расчёт Уровня Выполнения Договора (SLA)

17.1 Для проведения взаиморасчётов и общей оценки качества выполнения SLA Исполнителем производится расчёт показателя «Уровень выполнения SLA».

17.2 Исполнитель предоставляет Заказчику услуги с коэффициентом доступности 99,9 % в месяц. Интерфейс самообслуживания (%) - 98,0%

17.3 Периоды времени, в которые производятся согласованные с Заказчиком работы (плановые регламентные или аварийные), не являются случаями прерывания Услуги. Информация о плановых технических работах, предоставляется Заказчику в соответствии с Таблицей №2 - Перерывы и уведомления при оказании услуг Исполнителем. Общая продолжительность всех периодов времени, исключаемых из расчета SLA в соответствии с настоящим пунктом (плановые регламентные, срочные и аварийные работы), не может превышать 36 часов в год.

17.4 Исполнитель несёт ответственность исключительно за работу виртуальной инфраструктуры. Любые сбои в работе операционных систем, СУБД или прикладного ПО не связанные с работой виртуальной инфраструктуры, используемого заказчиком, не оказывают влияние на расчёт SLA по доступности сервиса. Ответственность за администрирование и восстановление в данном случае лежит исключительно в компетенции Заказчика.

17.5 Плановые регламентные и срочные работы проводятся исключительно после получения письменного утверждения от Заказчика. Заказчик имеет право мотивированно отклонить дату/время проведения работ и предложить их перенос на другую дату/время без применения к Заказчику каких-либо штрафных санкций.

17.6 Информация о плановых технических работах, проводимых вне стандартного времени регламентных работ (обслуживания), предоставляется не менее чем за 48 часов до начала работ.

17.7 Информация о срочных работах, проводимых вне стандартного времени регламентных работ (обслуживания), предоставляется не менее чем за 12 часов до начала работ.

17.8 Для согласования проведения плановых технических и срочных работ Исполнитель направляет план производства работ с указанием состава проводимых работ, времени, ответственного, контакты (телефон рабочий, телефон мобильный, электронную почту) ответственного за выполнение работ при оказании услуг и план восстановления на случай непредвиденных ситуаций.

17.9 Стороны соглашаются квалифицировать перерывы предоставления доступа к Услугам указанные Таблице №2 «Перерывы и уведомления при оказании услуг Исполнителем», как предоставление доступа к Услугам в штатном режиме

и не включать такие перерывы во время недоступности Услуг, а также перерывы, которые явились следствием: - изменения Заказчиком настроек программного обеспечения, прямо или косвенно влияющих на доступ к Услугам и/или аппаратное обеспечение, находящееся в зоне ответственности Исполнителя, производимые без согласования с Исполнителем; - нарушения Заказчиком условий Договора с Исполнителем в части обеспечения условий, необходимых для доступа к Услугам, в том числе условий оплаты; - неработоспособности или несовместимости программного обеспечения, используемого Заказчиком; - доступа третьих лиц к учетным данным Заказчика, произошедшего по вине Заказчика; - превышения Заказчиком максимально допустимой нагрузки на предоставленные вычислительные ресурсы (ГГц, Гб, IOPS); - обстоятельств непреодолимой силы, определённых согласно условий Договора.

17.10 Фактическая доступность предоставляемого ИТ-сервиса определяется по формуле: Фактическая доступность сервиса = (Т – Тавр)/Т*100%, (или отношение времени доступности сервиса к согласованному времени его предоставления за оцениваемый период), где: Т - согласованное время предоставления сервиса за оцениваемый период; Тавр - фактическое время, когда сервис был недоступен в течение согласованного времени его предоставления. Периоды времени, в которые производятся согласованные с Заказчиком работы при оказании услуг (плановые регламентные или срочные работы), не являются случаями недоступности услуги и определяются по таблице №2 (Перерывы и уведомления при оказании услуг Исполнителем). Факты недоступности ИТ сервиса актируются после выполнения работ по восстановлению работоспособности ИС Заказчика. Время начала недоступности ИТ сервиса вычисляется исходя из следующих документов: логи серверов/отчетов в системе мониторинга, в которых отразились события недоступности по локальной сети или сервисам, а также ИС Заказчика (в случае если это вызвано сбоем инфраструктуры VDC); несколько единичных заявок в БД Service-Desk с единой проблемой, подтверждённой далее в логах или открытием Проблемного билета. Время завершения недоступности вычисляется исходя из: логов восстанавливаемого сервера/отчетов в системе мониторинга (сервиса); факта доступности сервиса и ИС Заказчика с рабочих станций. Снижение платы (штрафные санкции) за несоответствие доступности сервиса рассчитываются в соответствии с размерами компенсаций, установленными в Таблице №3 Приложения №3 к настоящей Технической спецификации.

18. Распределение ответственности за защиту информации

18.1 Поставщик несет ответственность лишь за последствия, вызванные его действиями/бездействием.

Поставщик несёт ответственность за утечку, утрату, искажение, блокирование или несанкционированный доступ к информации Заказчика в случае, если соответствующее событие непосредственно вызвано ненадлежащим исполнением Поставщиком обязательств, прямо отнесённых настоящей Технической спецификацией к зоне ответственности и администрирования Поставщика.

Наличие инцидента само по себе не является основанием для возложения ответственности на Поставщика. При определении ответственности учитываются причина инцидента, зона ответственности каждой из Сторон и наличие прямой причинно-следственной связи между действиями или бездействием соответствующей Стороны и возникшими последствиями.

18.2 Поставщик не несёт ответственности за:

1. действия или бездействие Заказчика, его работников, представителей, подрядчиков либо иных лиц, получивших доступ к информационным ресурсам со стороны Заказчика;

2. использование, передачу или компрометацию учётных данных Заказчика, а также определёнными Заказчиком правами и уровнями доступа, произошедшие по прямой вине заказчика, при условии, что компрометация не была вызвана уязвимостями, сбоями или несанкционированным доступом на уровне инфраструктуры и сервисов Поставщика;

3. решения Заказчика относительно состава защищаемых и резервируемых объектов, расписание резервного копирования (за исключением внесения его в ПО Поставщиком), определение Заказчиком сроков хранения резервных копий, состава и содержания резервируемой информации и иных параметров;

4. параметры, правила, политики Firewall и иные конфигурационными решениями, установленные Поставщиком, в случае корректно исполненного Запроса Поставщиком;

5. архитектурные решения, конфигурации, операционные системы, базы данных, прикладные программные обеспечения и иные компоненты, администрирование которых не входит в зону ответственности Поставщика;

6. оборудование, каналы связи, программные обеспечения и иную инфраструктуру, находящуюся за пределами зоны ответственности Поставщика;

7. уязвимость программного или аппаратного обеспечения производителей и иных третьих лиц, включая ранее неизвестные уязвимости, при условии, выполнения Поставщиком предусмотренных настоящей Технической спецификацией мер защиты, реагирования, обновления и уведомления в пределах своей зоны ответственности;

8. невыполнение или несвоевременное выполнение Заказчиком предоставленных Поставщиком мотивированных письменных рекомендаций по устранению выявленных рисков информационной безопасности;

9. обстоятельства непреодолимой силы и иные обстоятельства, ответственность за которые в соответствии с Договором не возлагается на Поставщика.

18.3 Если Поставщик выполняет технические действия на основании задания, плана, параметров или Запроса Заказчика, Поставщик отвечает за корректность выполнения соответствующих технических действий в пределах предоставленного задания.

Приложение №1 Таблица №1 Определение приоритета инцидента

Приложение №2 Таблица №2 - Перерывы и уведомления при оказании услуг Исполнителем

Приложение №3 Таблица №3 - Доступность Услуги

Приложение №4 - Форма Запроса

**Приложение**

Приложение_№3_к_ТС_рус_каз.docx
Приложение №4 к ТС рус каз.docx
Приложение №2 к ТС рус каз.docx
Приложение №1 к ТС рус каз.docx

| | |
|---|---|
| Подписал | Ергалиев Равиль Лукпанович |
| Дата подписания | 23.11.2026 |