ТЕХНИКАЛЫҚ СИПАТТАМА

1264403 сатып алу бойынша
Ашық тендер тәсілімен

Лот № 1 (182 У, 4562325) Персоналды ұсыну бойынша қызметтер

Тапсырыс беруші: ЖШС "KAP Technology"
Ұйымдастырушы: ЖШС "KAP Technology"

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	182 У
Атауы және қысқаша сипаттамасы	Персоналды ұсыну бойынша қызметтер, Персоналды ұсыну бойынша қызметтер
Қосымша сипаттама	SAP ERP жүйесінде «Бюджеттік лимиттерді бақылау» функционалын дамыту жөніндегі жұмыстарды орындау үшін персоналды ұсыну
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Астана қ., г.Астана, ул.Сыганак, здание 17/12, 6-этаж
Жеткізу шарттары	-
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап 273 күнтізбелік күні
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 100%, Соңғы төлем - 0%

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

2. Қысқартулар мен анықтамалар

КО/Қоғам	«Қазатомөнеркәсіп» ұлттық атом компаниясы» акционерлік қоғамы
Тапсырыс беруші	«KAP Technology» ЖШС
О р ы н д а у ш ы , Мердігер	Шартқа сәйкес қызмет көрсететін тұлға
ЕТҰ	Еншілес және тәуелді ұйымдар
Жоба/Қызмет	SAP жүйелерін дамыту
SAP ERP, Жүйе	SAP Enterprise Resource Planning - SAP ECC 6.0 платформасында іске асырылған кәсіпорынды басқару жүйесі
SAP FM	Funds Management – бюджетті басқару
SAP BW, Жүйе	Business Warehouse – бизнес деректер қоймасы
АЖ	Ақпараттық жүйе

3. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

Осы Техникалық ерекшелік SAP ERP жүйесінде «Бюджет лимиттерін бақылау» фукнционалын дамыту жөніндегі міндеттерді орындау үшін персоналды ұсыну бойынша көрсетілетін қызметтердің (бұдан әрі - Қызмет) негізгі міндеттері мен талаптарын сипаттайды.

Функционалды дамыту SAP Funds Management-те (SAP FM) бюджеттік лимиттердің болуын белсенді бақылау (ББББ) тетігін жетілдіруді және оны міндеттемелерді қабылдауда қолдануды және нақты шығындарды көрсетуді қамтамасыз етуді көздейді. Қызмет көрсету шеңберінде SAP FM және SAP ERP сабақтас модульдерін жобалау, стандартты функционалдылығын теңшеу, қажетті функционалдық түзетулерді іске асыру, SAP BW/BPC-мен интеграциялау, есептілік пен талдауды іске асыру, пайдаланушылардың рөлдері мен өкілеттіктерін теңшеу, тестілеу жөніндегі жұмыстарды орындау көзделеді.

Міндеттерді орындау кезінде Орындаушы Тапсырыс беруші бекіткен жобалық шешімдерді басшылыққа алуы және функционалдылықтың іске асырылуын SAP стандартты функционалдылығының басым құралдарымен қамтамасыз етуі тиіс. Функционалдық пысықтаулар бекітілген жобалық шешім шеңберінде қажеттілік анықталған және SAP стандартты құралдарымен тиісті талапты іске асыру мүмкін болмаған жағдайда ғана орындалады. Функционалдық пысықтауларды орындау қажеттілігі болмаған жағдайда, Шарттың құны орындалуы қажеттілігі жоқ функционалдық пысықтаулардың құрамы мен көлемін ескере отырып, келісу нәтижелері бойынша Тараптар айқындайтын сомаға азайтылуға тиіс.

Функционалды іске асыру кезінде бюджеттік бақылаудың үздіксіздігін қамтамасыз етуге және пайдаланушылардың белгіленген бақылау тетігін, оның ішінде SAP ERP функционалдығымен көзделген баламалы операциялар, құжаттар, транзакциялар және өзге сценарийлер арқылы айналып өту мүмкіндіктерін болдырмауға ерекше назар аударылуы тиіс.

Сапалы нәтижелер алу және міндеттерді орындаудың тиісті деңгейі мақсатында Орындаушы Тапсырыс берушіні төмендегілерді қоса алғанда, білікті персоналмен уақтылы қамтамасыз етуге тиіс::

- Қызмет көрсету үшін Техникалық ерекшеліктердің № 1 қосымшасында сипатталған тарифтерге сәйкес білікті мамандарды ұсыну және білікті мамандарды Тапсырыс беруші келіседі. Орындаушының Қызметтің функционалдық көлемін толық орындауды қамтамасыз ету үшін SAP-тың қосымша білікті мамандарын тартуға құқығы бар, бұл ретте мұндай мамандарды тарту Тапсырыс беруші үшін қосымша шығындарға әкеп соқтырмауы тиіс. Қосымша персоналды тартуға байланысты шығындарды орындаушы шарттың жалпы құны шеңберінде қамтамасыз етуге тиіс;

- № 3 қосымшада мамандардың санаттарына және олардың біліктілігіне қойылатын талаптардың сипаттамасы;
- Қызмет функционалдық ерекшеліктерге/техникалық тапсырмаларға сәйкес жүзеге асырылады. Еңбек шығындарының көлемі № 1 қосымшада сипатталған тарифтермен есептеледі және Тапсырыс берушімен келісіледі;
- Жобаны іске асыру барысында Орындаушы Қазақстан Республикасының Еңбек кодексіне сәйкес еңбек шартын, азаматтық-құқықтық сипаттағы шартты және/немесе өзге де міндетті құжаттарды жасасу жолымен тартылған мамандармен еңбек қатынастарын заңды түрде ресімдеуі қажет. Орындаушының персоналы Қорды сатып алуды жүзеге асыру тәртібіне № 14 қосымшаға сәйкес жұмыстарды орындау/қызметтерді көрсету үшін маман ретінде тартуға келісім беруге тиіс;

4. Жобаның көлемі, мақсаттары мен міндеттері

Корпоративтік орталықта (КО) және ЕТҰ-да (жобаны іске асыру периметрінде корсетілген) міндеттемелерді қалыптастыруды және нақты шығындарды көрсетуді қоса алғанда, қаржы-шаруашылық қызметтің барлық кезеңдерінде бюджет қаражатының қолжетімділігін автоматтандырылған тексеруді қамтамасыз ететін SAP Funds Management (FM) модулі базасында бюджеттік лимиттерді басқару және бақылау тетігін енгізу, бұл бюджеттің орындалуын өтпелі автоматтандырылған бақылауды қамтамасыз етуге мүмкіндік береді.

Қызметті ұсыну нәтижесінде түпкілікті бизнес-пайдаланушыларға мынадай мүмкіндіктер мен пайда берілуі тиіс:

- міндеттемелерді қабылдауды және бекітілген бюджеттік лимиттерден тыс шығыстарды жүзеге асыруды болдырмау;
- бюджеттің атқарылуын автоматтандырылған бақылау және бюджеттік міндеттемелерді есепке алу есебінен бюджет қаражатын пайдалану тиімділігін арттыру;
- босатылатын үнемдеуді жедел қайта бөлу мүмкіндігін қамтамасыз ету;
- бақылау рәсімдерін орындауға және қол операцияларын пайдалануды қысқартуға кететін еңбек шығындарын азайту;
- бюджеттік басқару процестерінің ашықтығын және қолжетімді бюджеттік лимиттер туралы деректердің дұрыстығын арттыру.

Жобаны іске асыру периметрі

- «Қазатомөнеркәсіп» ҰАК» АҚ;
- «Казатомпром-SaUran» ЖШС;
- «Аппақ» ЖШС;

- «ОРТАЛЫҚ» ӨК» ЖШС;
- «РУ-6 «ЖШС;
- «Байкен-U «ЖШС;
- «Turanium» ЖШС («Қызылқұм» ЖШС).

5. Функционалдық көлем

Жобаның функционалдық көлемі осы техникалық ерекшелікке № 2 қосымшада санамаланған міндеттерді құрайды. Көрсетілген жұмыс осы функционалдық көлем шеңберінде орындалуы тиіс.

Бұл ретте функционалдық көлемнің 1/3 ағымдағы міндеттерге құнның өзгеруін ескермей қосылуы мүмкін. Тапсырыс беруші осы техникалық ерекшелікке № 2 қосымшаға сәйкес міндеттердің жалпы көлемінің 25% -ынан аспайтын көлемде міндеттер құрамына толықтырулар, өзгерістер енгізуі мүмкін.

Жоспар-кесте енгізілген өзгерістер мен толықтыруларды ескере отырып, жұмыстарды орындау процесінде жаңартылатын болады және барлық жаңартулар тараптармен келісілген мерзімде Тапсырыс берушімен келісілуі тиіс. Қажет болған жағдайда, жаңартылған Жоспар-кесте өзгерістер енгізілген сәттен бастап 5 жұмыс күнінен кешіктірілмей сол мерзімде бекіту үшін ұсынылуы тиіс.

6. Құжаттандыруға қойылатын талаптар

Қызмет көрсету шеңберінде мынадай құжаттаманы ұсыну қажет:

- мақсатты архитектура шешімінің дизайны;
- жобалық шешім;
- техникалық ерекшеліктер;
- баптаулар журналы;
- интеграцияның техникалық құжаттамасы;
- есеп беру нысандары альбомы
- рөлдер мен өкілеттіктер матрицасы
- ақпараттық жүйені пайдаланушының нұсқаулығы;
- тестілеу нәтижелері бойынша хаттама;
- оқыту жоспары мен хаттамасы;
- тасымалдау сұраныстардың тізімі;
- SAP FM функционалдылығының дайындық хаттамасы.

Форматы: MS Word, MS Excel, MS Power Point.

- Құжаттар Тапсырыс берушінің қабылдаған ішкі талаптарын ескере отырып, мемлекеттік және орыс тілдерінде әзірленеді. БҚ пайдаланушылар үшін құжаттама (көмек файлдары және пайдаланушылар нұсқаулары) сандық және қағаз түрінде ұсынылуы тиіс.
- Құжаттама (дайындауға Орындаушы жауапты) Тапсырыс берушіге электрондық

түрде Microsoft Office форматында, ал тараптармен бекітілген және келісілген құжаттар электрондық дискіге жүктеу арқылы Adobe PDF форматында берілуі тиіс.

7. Ақпараттық қауіпсіздік бойынша талаптар

Орындаушы шарт жасалған күннен бастап күнтізбелік 10 күн ішінде Тапсырыс берушімен құпиялылық туралы келісім жасауы және өз қызметкерлерін шартты орындау процесінде қызметкерлерге белгілі болған құпия мәліметтерді жария еткені үшін жауаптылығы туралы хабардар етуі, сондай-ақ шартты орындауға тартылған қызметкерлерден құпия мәліметтерді жария етпеу туралы дербес міндеттемелер алуы тиіс.

Қоғамның АТ-ресурстарына рұқсат берілген жағдайда, Орындаушының қызметкерлері «Қазатомөнеркәсіп» ҰАК» АҚ Ақпараттық қауіпсіздік саясатын және ақпараттық қауіпсіздік талаптарын сақтау туралы дербес міндеттемелерге қол қоюы тиіс.

Орындаушы қызмет көрсету кезінде Қоғамның және Тапсырыс берушінің нормаларын, ережелерін, нұсқаулықтарын, стандарттарын және басқа да нормативтік құжаттарын, ақпараттық қауіпсіздік талаптарына қатысты Қазақстан Республикасының нормативтік құқықтық актілерін басшылыққа алуы тиіс.

Орындаушы қызметтерді көрсету кезінде ақпараттық ресурстар мен жүйелердегі ақпараттың сақталуын, Тапсырыс беруші ақпаратының сақталуын, оның құпиялылығын қамтамасыз етуге, Тапсырыс берушіден алынатын құжаттардың сақталуын және құпиялылығын қамтамасыз етуге тиіс.

Корпоративтік желіден тыс қосылған жағдайда, Орындаушы үшін Қоғамның ақпараттық жүйесіне қолжетімділікті Қоғамның мультифакторлық сәйкестендіруі және Қоғамның АҚКЖ қажетті компоненттерін, оның ішінде РАМ-жүйелерін орнату арқылы VPN арқылы жүзеге асыруға, сондай-ақ тек қана арнайы бөлінген қолжетімділік нүктелері (Қоғамның терминалдық серверлері) арқылы жүзеге асыруға тиіс.

Жүйе жекелеген модульдермен және жекелеген есеп беру нысандарымен шектелмей, оқуға және (немесе) редакциялауға қатысты қол жеткізуді шектеу режимін автоматтандыруды қамтамасыз ететін тетіктерді пайдалануға мүмкіндік беруі тиіс.

Жүйе мыналарды қамтамасыз етуі тиіс:

- Логин және пароль көмегімен пайдаланушыны сәйкестендіргеннен кейін ғана Жүйеге қол жеткізуді ұсыну.
- Пайдаланушылардың санаттары, топтары бойынша қол жеткізу құқықтарының аражігін ажырату.
- Пайдаланушының жүйеге кіру немесе парольдерді таңдау арқылы осындай әрекеттердің әрбір жағдайына аудит (тіркеу).
- Пайдаланушы әрекеттерінің аудиті.

- Кез келген ақпараттық объектілерді құру, өзгерту, редакциялау, келісу, жою аудиті.
- SSL/HTTPS хаттамаларын пайдалана отырып, клиент пен жүйе сервері арасында берілетін ақпаратты шифрлауды пайдалану. SSL сертификаттарын Орындаушы ұсынады. SSL хаттамасындағы трафикті шифрлау үшін пайдаланылатын сертификаттар Қазақстан Республикасында сертификатталған және Қоғамда және ЕТҰ-да пайдалануға қабылданған крипто-провайдерлер мен алгоритмдерді пайдалануға тиіс.

Жүйе қоймадағы кез келген ақпараттық объектілерге қол жеткізу құқықтарының аражігін ажырату мүмкіндігін (рөлдік модельді пайдалану), пайдаланушылар деңгейінде қол жеткізу құқықтарының аражігін ажырату мүмкіндігін қолдауға тиіс.

Жүйенің серверлік аппараттық және бағдарламалық қамтылымы, сондай-ақ техникалық құралдардың бүкіл кешені Орындаушы мен Тапсырыс беруші арасында жеке айтылған жағдайларды қоспағанда, тұрақты жұмыс істеуі тиіс.

Жүйенің барлық серверлерінде Қоғамның АҚКЖ-ның өзекті және міндетті компоненттері орнатылуы тиіс.

Клиенттік бағдарламалық қамтылым және пайдаланушылар мен жүйе әкімшісінің техникалық құралдары Орындаушы мен Тапсырыс беруші арасында жеке ескертілетін жағдайларды қоспағанда, жұмыс уақытында қолжетімді болуы тиіс.

Төтенше жағдайлар кезінде жүйе мыналарды қамтамасыз етуі керек:

- деректердің сақталуы;
- ағымдағы транзакциялардың аяқталуы және деректердің тұтастығы;
- Жүйенің барлық құрамдас бөліктерінің жұмысын бүтіндігін бұзбай аяқтау мүмкіндігі;

Жүйенің немесе инфрақұрылымның жұмысы бұзылған жағдайда ақпаратты сақтау үшін жүйеде резервтік көшіру тетігі болуы тиіс. Резервтік көшіру сервердегі автоматты режимде де, жүйе әкімшісі тікелей жұмыс орнында іске қосатын қолмен де көзделуі тиіс.

Ақпараттық қауіпсіздікті қамтамасыз ету үшін Орындаушы мыналарды қамтамасыз етуі тиіс::

төмендегілерді талап ететін сәйкестендіруді басқару:

- пайдаланушылар мен артықшылықты пайдаланушыларды сәйкестендіру;
- бір технологиялық платформа шегінде пайдаланушыларды федеративтік сәйкестендіру;
- пайдаланушының сәйкестендіргіші жойылғаннан кейін сәйкестендіру туралы ақпаратты сақтау;

- пайдаланушының өкілеттік бейіндерін тағайындау рәсімдерін бақылау құралдарын қолдану.

төмендегілерді талап ететін кіруді басқару:

- ақпараттық жүйе әкімшісі мен виртуалдандыру ортасы әкімшісінің өкілеттіктерін бөлу;
- виртуалдандыру ортасы әкімшісінің пайдаланушының деректеріне қол жеткізу құқықтарын шектеу. Қол жеткізу құқықтары ақпараттық қауіпсіздіктің техникалық құжаттамасында және қызмет көрсету туралы сервистік келісімде айқындалған нақты рәсімдермен шектеледі және ұдайы өзектендіруге жатады;
- барлық өкілеттіктері бар рөлдерді пайдалануды шектеу. Ақпараттық жүйе әкімшісінің профайлын баптау виртуалдандыру ортасының компоненттеріне қол жеткізуді болдырмайды;
- ең аз артықшылықтарды айқындау және қол жеткізуді рөлдік басқару моделін іске асыру;
- қорғалған шлюз немесе жіберушілердің рұқсат етілген желілік мекенжайларының тізімі арқылы қашықтан қол жеткізу.

Орындаушы төмендегілерді қолдана отырып, қол жеткізуді бақылау мүмкіндігін қамтамасыз етуі керек:

- пайдаланушылардың құпия сөздерін сәйкестендіру, сәйкестендіру және басқару;
- сәтті және сәтсіз қол жеткізуді тіркеу;
- жүйелік артықшылықтарды пайдалануды тіркеу;
- қажет болған жағдайда қосылу уақытын шектеу және уақыт лимитін арттыру бойынша сеансты бұғаттау;
- Пайдаланушылар үшін ерекшеліктер және операциялық жүйенің бақылау құралдарын айналып өтуге қабілетті жүйелік утилиттерді пайдалану әкімшілері үшін шектеулер.

Орындаушы ақпараттық қауіпсіздік инциденттерін жинау және талдау жүйесіне (SIEM) беру үшін қажетті деректерді теңшеу және жинау бойынша консультациялық және техникалық көмекті қамтамасыз етуге тиіс.

7.1. Рұқсатсыз кіруден қорғауға қойылатын талаптар

Рұқсатсыз кіруден қорғау мыналарды қамтамасыз етуі керек:

- пайдаланушының атын (логинін) және паролін тексеру негізінде пайдаланушыны сәйкестендіру;
- тиісті рұқсаттардың болуын талап ететін Жүйенің ақпараттық-есептеу ресурстарына қол жеткізу үшін пайдаланушыны авторизациялау;

- пайдаланушылардың деректерді енгізуге, түзетуге, қарауға құқықтарын дербестендірілген анықтау;
- пайдаланушылардың жүйелік ресурстарға қол жеткізу құқықтарын дербестендірілген анықтау;
- Жүйеде пайдаланушылардың жұмысын хаттамалау.

Рұқсат етілмеген кіруден қорғаудың базалық құралдары ретінде мыналар қолданылуы тиіс:

- операциялық жүйені және деректер базасын басқару жүйесін (ДББЖ) әкімшілендіру құралдары;
- Жүйеде пайдаланушыларды топтарға бөлу функцияларын іске асыру және оларға ақпаратты рұқсатсыз жоюды, алуды, модификациялауды болдырмау үшін тиісті қол жеткізу құқықтарын беру;
- деректердің физикалық деңгейіндегі қорғалған байланыс арналары.

Ақпаратты рұқсатсыз кіруден қорғау, сондай-ақ дерекқор сервері орналасқан үй-жайларға бөгде адамдардың кіруін болдырмайтын ұйымдастыру шараларымен қамтамасыз етілуі тиіс.

Жүйенің ақпаратын рұқсатсыз қол жеткізуден қорғау әдістемесі жаңа технологияларды игеру шамасына қарай өзгеруі мүмкін.

Орындаушы «Ақпараттандыру туралы» Қазақстан Республикасы Заңының, «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасы Заңының, сондай-ақ ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды белгілейтін нормативтік құқықтық актілердің талаптарын қоса алғанда, бірақ олармен шектелмей, Қазақстан Республикасының қолданыстағы заңнамасына қатаң сәйкестікте қызметтер көрсетуге міндетті.

Орындаушы ISO/IEC 27001 (қолданылуы болған кезде) қоса алғанда, ақпараттық қауіпсіздік саласындағы халықаралық стандарттардың, сондай-ақ ақпараттық қауіпсіздік бөлігінде Қоғамның ішкі нормативтік құжаттары мен талаптарының сақталуын қамтамасыз етуге міндетті.

Тапсырыс берушінің деректерін сақтау, өңдеу және беру Қазақстан Республикасының дербес деректер туралы заңнамасының талаптарына сәйкес жүзеге асырылуға тиіс. Тапсырыс берушінің дербес деректері және (немесе) өзге де ақпараты бар дерекқорлар Қазақстан Республикасының аумағында орналастыруға жатады.

Орындаушы қызмет көрсетудің барлық мерзімі ішінде көрсетілген талаптардың сақталуына жауапты болады.

7.2. Ақпараттың сақталуына қойылатын талаптар

Авариялар кезінде ақпараттың сақталуы жөніндегі талаптар және істен шығулардың, сондай-ақ жұмыстағы іркілістер мен авариялық жағдайлардың есептік түрлері Жүйеге қойылатын жалпы техникалық талаптармен айқындалуы тиіс. Бұл ретте әкімшінің мамандандырылған бағдарламалық құралдары мыналарды қамтамасыз етуге тиіс:

- Істен шығу жағдайларының туындауы нәтижесінде жұмыс қабілеттілігі мен деректерін толық қалпына келтіру мүмкіндігі;
- Кейіннен қалпына келтіре отырып, сақтаудың резервтік құрылғыларына деректерді қайталау жүйесінің болуы.
- Қауіпсіздік құралдары тұтастай алғанда жүйенің жоғары істен шығуға төзімділігін қамтамасыз етуі, мынадай функциялардың орындалуын көздеуі тиіс:
- Зиянды бағдарламалардан қорғауды қамтамасыз ету;
- Жергілікті желілерден де, сырттан да рұқсатсыз кіруден қорғауды қамтамасыз ету.

7.3. Ақпарат беруге қойылатын талаптар

Ақпарат беруге қойылатын негізгі талаптар:

- Құпия ақпарат ашық сыртқы байланыс арналары (Интернет) арқылы қорғалмаған түрде берілмеуге тиіс;
- Сыртқы ұйымдармен ақпарат алмасу тараптар арасында ресми жасалған «Құпиялылық туралы келісіммен» (NDA) реттелуі тиіс.

Деректерді беру кезінде осы талаптарға қол жеткізу деректерді шифрлау жолымен қамтамасыз етіледі.

7.4. Дербес деректерге қойылатын талаптар

ҚР «Дербес деректер және оларды қорғау туралы» Заңының 7-бабына сәйкес дербес деректерді өңдеу нақты, алдын ала анықталған және заңды мақсаттарға жетумен шектелуі тиіс. Дербес деректерді жинау мақсаттарымен үйлеспейтін дербес деректерді өңдеуге жол берілмейді. Мазмұны мен көлемі оларды өңдеу мақсаттарына қатысты артық болып табылатын дербес деректер өңдеуге жатпайды.

ҚР «Дербес деректер және оларды қорғау туралы» Заңының 17-бабына сәйкес статистикалық, әлеуметтік, ғылыми, маркетингтік зерттеулер жүргізу үшін дербес деректерді жинау, өңдеу кезінде меншік иесі, сондай-ақ дербес деректерді беретін үшінші тұлға дербес деректерді жинау, өңдеу қағидаларына сәйкес оларды иесіздендіруге міндетті.

7.5. Ортаға қойылатын талаптар

Орындаушы өнімді, тестілік және әзірлеу ортасын бөлуді мынадай қағидаларға сәйкес пайдалануы тиіс:

- Әзірлеу ортасы жүйені әзірлеу және оған өзгерістер енгізу үшін ғана қызмет етеді;
- Тестілік орта қателердің болмауына ақпараттық жүйедегі өзгерістерді тестілеу жұмыстарын орындау, бастамашының талаптарына сәйкестікті сақтау және жұмыс нәтижесін бастамашыға көрсету үшін ғана қызмет етеді;
- Бастамашы бекіткен өзгерістер ғана өнімді ортаға көшіріледі;
- Жұмыс және түрлендіру олардың көшірмелерімен жүргізілуі тиіс;
- Ақпараттық жүйені әзірлеушілердің Қоғамның ақпараттық жүйесінің өнімді ортасына қолжетімділігі болмауы тиіс.

7.6. Журналға жазуға қойылатын талаптар

Журналға жазылатын БҚ оқиғаларының түрлері:

- Жүйедегі жүйелер мен процестерді іске қосу/тоқтату;
- Пайдаланушыларды авторизациялау (кіру және шығу), авторизациялаудың табысты және сәтсіз әрекеттері;
- Пайдаланушының сәтсіз немесе бас тартылған іс-әрекеттері;
- Пайдаланушының қол жеткізу объектілеріне қол жеткізуі;
- Қолданбалы БҚ пайдаланушылардың іс-әрекеттері (объектіге (деректерге) қол жеткізу, объектіні (деректерді) өзгерту, объектіні (деректерді) жою);
- «Қазатомөнеркәсіп «ҰАК «АҚ ақпараттық жүйелерін енгізу, әзірлеу, жаңғырту кезіндегі ақпараттық қауіпсіздік жөніндегі талаптар» нұсқаулығына сәйкес басқа да оқиғалар.

7.7. Өзге талаптар

Сервистерді және/немесе АЖ жалпы жаңғыртылған жағдайда, «Қазатомөнеркәсіп» ҰАК» АҚ ақпараттық жүйелерін енгізу, әзірлеу, жаңғырту кезіндегі ақпараттық қауіпсіздік жөніндегі талаптар» нұсқаулығына сәйкес ақпараттық қауіпсіздік жөніндегі талаптар орындалуға тиіс.

8. Эргономикаға және техникалық эстетикаға қойылатын талаптар

Жүйе эргономикаға қойылатын мынадай талаптарға сәйкес келуге тиіс:

- Пайдаланушы интерфейсі тиімділік пен эргономикалықтың талаптарын қанағаттандыруы тиіс: ақпаратты адам қабылдауы үшін мүмкіндігінше тиімді

бейнелеу және экранда бейнелеуді түстік гамманы, элементтерді, пиктограммаларды, дыбыстарды, анимацияны қолдану бойынша оңтайлы шешім арқылы ақпараттың ең маңызды бірліктеріне назар аударатындай етіп құрылымдау.

- Жұмыс экрандарындағы барлық пиктограммалар міндетті түрде олардың мақсатын түсіндіретін және пиктограмманың ортасына курсор орнату кезінде экранда ашылатын жазбалармен жабдықталуы тиіс. Пиктограммалардың графикалық бейнеленуі интуитивті түсінікті болуы және қандай да бір объектіні таңдау немесе оған әрекет ету кезінде оның не екені туралы ақпаратты қамтуы тиіс. Пайдаланушының есептерді шешудің әртүрлі кезеңдерінде ақпаратты бейнелеудің көрнекі құралы болуы қажет, ол оның іс-қимылының экранда орналасқан объектілерге қалай әсер ететінін көруі тиіс.
- Жүйенің экрандық нысандарының өрістері анықтамалықтардан мәндерді таңдау жолымен Жүйені пайдаланушылармен толтырылуы тиіс. Ашылатын тізімдердің ені деректерге бейімделуі керек, егер бүкіл тізім сәйкес келмесе, ұзындығы ұқсас не жүйенің жұмыс терезесінің төменгі шегіне дейін болуы керек.
- Жүйе интерфейсі пайдаланушылардың жұмыс орындарында пайдаланылатын экрандардың барлық рұқсаттарын қолдауы тиіс.
- Жүйені пайдаланушылар Жүйенің бағдарламалық қамтамасыз етуінің стандартты функционалдығын пайдалана отырып, Жүйеде орыс және ағылшын тілдерінде іздестіруді жүзеге асыру мүмкіндігіне ие болуы тиіс.
- Жүйе Жүйенің әртүрлі компоненттері арасында өту кезінде бір реттік авторизациялау (single sign-on) мүмкіндігін қамтамасыз етуі тиіс.
- Жоспарлау мақсаттары үшін Жүйенің негізгі интерфейсі MS Excel болып табылады. Бұл ретте жүйенің функцияларына Web-интерфейс арқылы қашықтан қол жеткізу мүмкіндігі қамтамасыз етілуі тиіс (кем дегенде 8 және 9-нұсқалардың IE шолғышын қолдайды). Бюджеттік процестің мәртебесін келісу және басқару функционалдығы Web-интерфейс түрінде іске асырылуы тиіс.
- Есептермен жұмыс істеу кезінде сұрыптауды, топтауды, сүзуді орындау мүмкіндігі көзделуі тиіс.
- Жүйеде MS Excel файлдарынан және/немесе жазық файлдардан (CSV) деректерді жүктеудің штаттық құралдары болуы тиіс.
- Жүйе деректерді «мәтінді санға» түрін одан әрі түрлендіруді талап етпейтін Excel-форматында экспорттау мүмкіндігіне ие болуы тиіс, сондай-ақ түсірілетін деректер sum if, v (h) lookup түріндегі функциялармен және Excel жиынтық кестелерімен кейіннен сұрыптауға, сүзуге және өңдеуге барынша бейімделуі тиіс.
- Алдын ала жасалған есептерден басқа оларды сақтау мүмкіндігі бар еркін есептерді құрастыру үшін конструктор қажет. Ерікті есептерді жүйенің негізгі пайдаланушысы жасауы мүмкін және әзірлеушілерді тартуды талап етпеуі тиіс.

9. Орындаушыға қойылатын талаптар

Орындаушы SAP PCoE серіктесі ретінде жарамды мәртебеге ие болуы керек және тендерлік өтінімде жарамды SAP PCoE сертификатын растайтын сертификаттың көшірмесін ұсынуы керек.

Қосымша

Қосымша 1 к ТЕ (тариф)260826.docx
Қосымша 3 к ТЕ (Біліктілік талаптары).docx
Приложение 3 к ТС (квалификационные требования).docx
Приложение 2 к ТС (перечень задач).docx
Қосымша 2 к ТЕ (тапсырмалар тізімі)26082026.docx
Приложение 1 к ТС (тариф).docx

Қол қойған	Шумаков Алибек Бейбитович
Қол қойылған күні	21.10.2026

Құжат «Самұрық-Қазына» АҚ сатып алу веб-порталымен құрылған
Документ сформирован веб-порталом закупок АО «Самрук-Қазына»

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1264403
способом Открытый тендер

Лот № 1 (182 У, 4562325) Услуги по предоставлению персонала

Заказчик: Товарищество с ограниченной ответственностью "KAP Technology"
Организатор: Товарищество с ограниченной ответственностью "KAP Technology"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	182 У
Наименование и краткая характеристика	Услуги по предоставлению персонала, Услуги по предоставлению персонала
Дополнительная характеристика	Услуги по предоставлению персонала для выполнения работ по развитию функционала «Контроль бюджетных лимитов» в системе SAP ERP
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Астана, г.Астана, ул.Сыганак, здание 17/12, 6-этаж
Условия поставки	-
Срок поставки	С даты подписания договора в течение 273 календарных дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 100%, Окончательный платеж - 0%

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

2. Сокращения и определения

КЦ/Общество	Акционерное общество «Национальная атомная компания «Казатомпром»
Заказчик	ТОО «KAP Technology»
Исполнитель, Подрядчик	Лицо, оказывающее услуги в соответствии с Договором
ДЗО	Дочерние и зависимые организации
Проект/Услуга	Развития систем SAP
SAP ERP, Система	SAP Enterprise Resource Planning - Система управления предприятием, реализованная на платформе SAP ECC 6.0
SAP FM	Funds Management –управление бюджетом
SAP BW, Система	Business Warehouse – бизнес хранилище данных
ИС	Информационная система

3. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

Настоящая Техническая спецификация описывает основные задачи и требования к предоставляемым услугам по

предоставлению персонала для выполнения задач по развитию фукнционала «Контроль бюджетных лимитов» в системе SAP ERP (далее – Услуга).

Развитие функционала предусматривает совершенствование механизма активного контроля наличия бюджетных лимитов (АКН) в SAP Funds Management (SAP FM) и обеспечение его применения в принятия обязательств и отражения фактических затрат. В рамках оказания Услуги предусматривается выполнение работ по проектированию, настройке стандартной функциональности SAP FM и смежных модулей SAP ERP, реализации необходимых функциональных доработок, интеграции с SAP BW/BPC, реализации отчетности и аналитики, настройке ролей и полномочий пользователей, тестированию.

При выполнении задач Исполнитель должен руководствоваться утвержденными Заказчиком проектными решениями и обеспечивать реализацию функциональности преимущественно средствами стандартной функциональности SAP. Функциональные доработки выполняются только в случае выявления потребности в рамках утвержденного проектного решения и невозможности реализации соответствующего требования стандартными средствами SAP. В случае отсутствия необходимости в выполнении функциональных доработок стоимость Договора подлежит уменьшению на сумму, определяемую Сторонами по результатам согласования с учетом состава и объема функциональных доработок, необходимость в выполнении которых отсутствует.

Особое внимание при реализации функционала должно быть уделено обеспечению непрерывности бюджетного контроля и исключению возможностей обхода установленного механизма контроля пользователями, в том числе посредством альтернативных операций, документов, транзакций и иных сценариев, предусмотренных функциональностью SAP ERP.

В целях получения качественных результатов и надлежащего уровня выполнения задач Исполнитель должен своевременно обеспечить Заказчика квалифицированным персоналом, включая нижеследующие:

- Предоставить квалифицированных специалистов для Услуги согласно тарифам, описанным в Приложении № 1 к Технической спецификаций, и квалифицированные специалисты согласовывается Заказчиком. Исполнитель имеет право привлекать дополнительных квалифицированных специалистов SAP для обеспечения полного выполнения функционального объема Услуги, при этом привлечение таких специалистов не должно влечь за собой дополнительных затрат для Заказчика. Затраты, связанные с привлечением дополнительного персонала, должны быть обеспечены исполнителем в рамках общей стоимости договора;
- Описание требований к категориям специалистов и их квалификации в Приложении № 3;
- Услуга осуществляется согласно функциональным спецификациям/ техническим заданиям. Объем трудозатрат высчитывается тарифами, описанными в Приложении № 1, и согласовывается Заказчиком;
- В ходе реализации проекта Исполнителю необходимо юридически оформить трудовые отношения с привлеченными специалистами путем заключения трудового договора, договора гражданско-правового характера и/или иных обязательных документов в соответствии с Трудовым кодексом Республики Казахстан. Персонал Исполнителя должен предоставить согласие на привлечение в качестве специалиста для выполнения работ/оказания услуг согласно Приложение № 14 к Порядку осуществления закупок Фонда;

4. Объем, цели и задачи проекта

Внедрение в Корпоративном центре (КЦ) и ДЗО (перечисленные в периметре реализации проекта) механизма управления и контроля бюджетных лимитов на базе модуля SAP Funds Management (FM), обеспечивающего автоматизированную проверку доступности бюджетных средств на всех этапах финансово-хозяйственной деятельности, включая формирование обязательств и отражение фактических затрат, что позволит обеспечить сквозной автоматизированный контроль исполнения

бюджета.

В результате предоставления Услуги конечным бизнес-пользователям должны быть предоставлены следующие возможности и выгоды:

- предотвращение принятия обязательств и осуществления расходов сверх утвержденных бюджетных лимитов;
- повышение эффективности использования бюджетных средств за счет автоматизированного контроля исполнения бюджета и учета бюджетных обязательств;
- обеспечение возможности оперативного перераспределения высвобождаемой экономии;
- снижение трудозатрат на выполнение контрольных процедур и сокращении использования ручных операций;
- повышение прозрачности процессов бюджетного управления и достоверности данных о доступных бюджетных лимитах.

Периметр реализации Проекта

- АО «НАК «Казатомпром»;
- ТОО «Казатомпром-SaUran»;
- ТОО «Аппак»;
- ТОО «ДП ОРТАЛЫК»;
- ТОО «РУ-6»;
- ТОО «Байкен-U»;
- ТОО «Turanium» (ТОО «Кызылкум»).

5. Функциональный объем

Функциональный объем проекта составляет задачи, перечисленные в Приложении №2 к настоящей технической спецификации. Указанные работы должны быть выполнены в рамках этого функционального объема.

При этом 1/3 функционального объема может быть добавлена к текущим задачам, без учета изменения стоимости. Заказчиком могут быть внесены дополнения, изменения к составу задач в объеме, не превышающем 25% от общего объема задач согласно Приложению №2 к настоящей технической спецификации.

План-график будет обновляться в процессе исполнения работ с учетом внесенных изменений и дополнений, и все обновления должны быть согласованы с Заказчиком в сроки, согласованные сторонами. В случае необходимости, обновленный План-график должен быть предоставлен для утверждения в те же сроки не позднее 5 рабочих дней с момента внесения изменений.

6. Требования к документированию

В рамках оказания Услуги необходимо предоставить следующую документацию:

- дизайн целевой архитектуры решения;
- проектное решение;
- технические спецификации;
- журнал настроек;
- техническая документация интеграции;

- альбом отчетных форм
- матрица ролей и полномочий
- руководство (инструкция) пользователя информационной системы;
- протокол по результатам тестирования;
- план и протокол обучения;
- список транспортных запросов;
- протокол готовности функциональности SAP FM.

Формат: MS Word, MS Excel, MS Power Point.

- Документы разрабатываются на государственном и русском языках с учетом принятых внутренних требований Заказчика. Документация для пользователей ПО (файлы помощи и руководства пользователей) должна быть предоставлена в цифровом и бумажном виде.
- Документация (за подготовку несет ответственность Исполнитель) должна быть передана Заказчику в электронном виде в формате Microsoft Office, а утверждённые и согласованные сторонами документы в формате Adobe PDF, путем выгрузки на электронный диск.

7. Требования по информационной безопасности

Исполнитель должен в течение 10 календарных дней с даты заключения договора заключить с Заказчиком соглашение о конфиденциальности и уведомить своих работников об ответственности за разглашение конфиденциальных сведений, ставших известными работникам в процессе исполнения договора, а также взять с работников, привлеченных к исполнению договора, персональные обязательства о неразглашении конфиденциальных сведений.

В случае предоставления доступа к ИТ-ресурсам Общества, работники Исполнителя должны подписать персональные Обязательства о соблюдении Политики информационной безопасности АО «НАК «Казатомпром» и требований информационной безопасности.

Исполнитель при оказании услуг должен руководствоваться нормами, правилами, инструкциями, стандартами и другими нормативными документами Общества и Заказчика, нормативными правовыми актами Республики Казахстан, касающимися требований информационной безопасности.

Исполнитель при оказании услуг должен обеспечить сохранность информации, находящейся в информационных ресурсах и системах, сохранность информации Заказчика, ее конфиденциальность, обеспечивать сохранность и конфиденциальность документов, получаемых от Заказчика.

В случае подключения вне корпоративной сети, доступ для Исполнителя к информационным система Общества должно осуществлять посредством VPN с мультифакторной аутентификации Общества и установкой необходимых компонентов КСИБ Общества, в том числе PAM-систем, а также осуществлять исключительно посредством специально-выделенных точек доступа (терминальные серверы Общества).

Система должна позволять использование механизмов, обеспечивающих автоматизацию режима ограничения доступа по чтению и (или) редактированию в отношении, но не ограничиваясь отдельными модулями и отдельными отчетными формами.

Система должна обеспечивать:

- Предоставление доступа к Системе только после идентификации пользователя с помощью логина и пароля.
- Разграничение прав доступа по категориям, группам пользователей.

- Аудит (фиксация) каждого случая вхождения пользователя в систему или попыток такового путем подбора паролей.
- Аудит действий пользователя.
- Аудит создания, изменения, редактирования, согласования, удалении любых информационных объектов.
- Использование шифрования информации, передаваемой между клиентом и сервером системы, с использованием протоколов SSL/HTTPS. Сертификаты SSL предоставляются Исполнителем. Сертификаты, используемые для шифрования трафика в протоколе SSL, должны использовать крипто-провайдеры и алгоритмы, сертифицированные в Республики Казахстан и принятые к использованию в Обществе и ДЗО.

Система должна поддерживать возможность разграничения прав доступа к любым информационным объектам в хранилище (использование ролевой модели), возможность разграничения прав доступа на уровне пользователей.

Серверное аппаратное и программное обеспечение Системы, а также весь комплекс технических средств должны постоянно функционировать за исключением случаев, отдельно оговариваемых между Исполнителем и Заказчиком.

На всех серверах Системы должны быть установлены актуальные и обязательные компоненты КСИБ Общества.

Клиентское программное обеспечение и технические средства пользователей и администратора системы должны быть доступны в рабочее время, за исключением случаев, отдельно оговариваемых между Исполнителем и Заказчиком.

При аварийных ситуациях Система должна обеспечивать:

- сохранность данных;
- завершение текущих транзакций и целостность данных;
- возможность завершения работы всех компонентов Системы без нарушения целостности;

Для сохранения информации в случае нарушения работы Системы, либо инфраструктуры, система должна обладать механизмом резервного копирования. Резервное копирование должно предусматриваться как в автоматическом режиме на сервере, так и в ручном, запускаемом непосредственно на рабочем месте администратором системы.

Для обеспечения информационной безопасности Исполнитель должен обеспечить:

управление идентификацией, требующее:

- аутентификацию пользователей и привилегированных пользователей;
- федеративной идентификации пользователей в пределах одной технологической платформы;
- сохранения информации об аутентификации после удаления идентификатора пользователя;
- применения средств контроля процедур назначения профилей полномочий пользователя.

управление доступом, требующее:

- разделения полномочий администратора информационной системы и администратора среды виртуализации;
- ограничения прав доступа администратора среды виртуализации к данным пользователя. Права доступа ограничиваются конкретными процедурами, определенными в технической документации информационной безопасности и сервисном соглашении об обслуживании, и подлежат регулярной актуализации;
- ограничения использования ролей со всеми полномочиями. Настройки профиля администратора

информационной системы исключают получение доступа к компонентам среды виртуализации;
- определения минимальных привилегий и реализацию модели ролевого управления доступом;
- удаленного доступа посредством защищенного шлюза или списка разрешенных сетевых адресов отправителей.

Исполнитель должен обеспечить возможность контроля доступа с применением:

- идентификации, аутентификации и управления паролями пользователей;
- регистрации успешных и неудавшихся доступов;
- регистрации использования системных привилегий;
- ограничения времени соединения, при необходимости, и блокировки сеанса по превышению лимита времени;
- исключения для пользователей и ограничения для администраторов использования системных утилит, способных обходить средства контроля операционной системы.

Исполнитель должен обеспечить консультационную и техническую помощь по настройке и сбору необходимых данных для передачи их в систему сбора и анализа инцидентов информационной безопасности (SIEM).

7.1. Требования к защите от несанкционированного доступа

Защита от несанкционированного доступа должна обеспечивать:

- идентификацию пользователя на основе проверки имени (логина) пользователя и пароля;
- авторизацию пользователя для доступа к информационно-вычислительным ресурсам Системы, требующим наличия соответствующих разрешений;
- персонифицированное определение прав пользователей на ввод, корректировку, просмотр данных;
- персонифицированное определение прав пользователей на доступ к системным ресурсам;
- протоколирование работы пользователей в Системе.

В качестве базовых средств защиты от несанкционированного доступа должны использоваться:

- средства администрирования операционной системы и системы управления базами данных (СУБД);
- реализация в Системе функций распределения пользователей по группам и присвоение им соответствующих прав доступа для предотвращения несанкционированного удаления, съема, модификации информации;
- защищенные каналы связи на физическом уровне данных.

Защита информации от несанкционированного доступа также должна обеспечиваться организационными мерами, предотвращающими доступ посторонних лиц в помещения, где находится сервер базы данных.

Методика защиты информации Системы от несанкционированного доступа может изменяться по мере освоения новых технологий.

Исполнитель обязан оказывать услуги в строгом соответствии с действующим законодательством Республики Казахстан, включая, но не ограничиваясь, требованиями Закона Республики Казахстан «Об информатизации», Закона Республики Казахстан «О персональных данных и их защите», а также нормативных правовых актов, устанавливающих единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности.

Исполнитель обязан обеспечить соблюдение международных стандартов в области информационной безопасности,

включая ISO/IEC 27001 (при наличии применимости), а также внутренних нормативных документов и требований Общества в части информационной безопасности.

Хранение, обработка и передача данных Заказчика должны осуществляться в соответствии с требованиями законодательства Республики Казахстан о персональных данных. Базы данных, содержащие персональные данные и (или) иную информацию Заказчика, подлежат размещению на территории Республики Казахстан.

Исполнитель несет ответственность за соблюдение указанных требований на протяжении всего срока оказания услуг.

7.2. Требования к сохранности информации

Требования по сохранности информации при авариях и расчетные типы отказов, а также сбоев в работе и аварийных ситуаций должны определяться общими техническими требованиями к Системе. При этом специализированные программные средства администратора должны обеспечивать:

- Возможность полного восстановления работоспособности и данных в результате возникновения сбойных ситуаций;
- Наличие системы дублирования данных на резервные устройства хранения с последующим восстановлением.
- Средства безопасности должны обеспечить высокую отказоустойчивость системы в целом, предусматривать выполнение следующих функций:
- Обеспечение защиты от вредоносных программ;
  Обеспечение защиты от несанкционированного доступа, как из вне, так и из локальных сетей.

7.3. Требования к передаче информации

Основные требования к передаче информации:

- Конфиденциальная информация не должна передаваться в незащищенном виде по открытым внешним каналам связи (Интернет);
- Обмен информацией с внешними организациями должен регулироваться официально заключенным между сторонами «Соглашением о конфиденциальности» (NDA).

При передаче данных, достижение данных требований обеспечивается путем шифрования данных.

7.4. Требования к персональным данным

Согласно статье 7 Закона РК «О персональных данных и их защите», Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Не подлежат обработке персональные данные, содержание и объем которых являются избыточными по отношению к целям их обработки.

Согласно статьи 17 Закона РК «О персональных данных и их защите», при сборе, обработке персональных данных для проведения статистических, социологических, научных, маркетинговых исследований собственник, а также третье лицо, передающие персональные данные, обязаны их обезличить в соответствии с правилами сбора, обработки персональных данных.

7.5. Требования к средам

Исполнитель должен использовать разделение продуктивной, тестовой и среды разработки, согласно следующим правилам:

- Среда разработки служит только для разработки и внесения изменений в систему;
- Тестовая среда служит только для выполнения работ тестирования изменений информационной системы на отсутствие ошибок, соблюдения соответствия требованиям инициатора и демонстрации результата работ инициатору;
- Только утверждённые инициатором изменения переносятся в продуктивную среду;
- Работа и модификация должна проводиться с их копиями;
- Разработчики информационной системы не должны иметь доступ к продуктивным средам информационной системы Общества.

7.6. Требования к журналированию

Типы событий ПО, подлежащие журналированию:

- Запуск/остановка системы и процессов в системе;
- Авторизация (вход и выход) пользователей, успешные и неуспешные попытки авторизации;
- Неудавшиеся или отвергнутые действия пользователя;
- Получение пользователем доступа к объектам доступа;
- Действия пользователей прикладного ПО (доступ к объекту (данным), изменения объекта (данных), удаления объекта (данных));
- Другие события согласно Инструкции «Требования по информационной безопасности при внедрении, разработке, модернизации информационных систем АО «НАК «Казатомпром».

7.7. Иные требования

В случае модернизации сервисов и/или ИС в целом, должны быть выполнены требования по информационной безопасности согласно Инструкции «Требования по информационной безопасности при внедрении, разработке, модернизации информационных систем АО «НАК «Казатомпром».

8. Требования к эргономике и технической эстетике

Система должна соответствовать следующим требованиям к эргономике:

- Пользовательский интерфейс должен удовлетворять требованиям эффективности и эргономичности: отображать

информацию настолько эффективно, насколько это возможно для человеческого восприятия и структурировать отображение на экране таким образом, чтобы привлечь внимание к наиболее важным единицам информации посредством оптимального решения по применению цветовой гаммы, компоновки элементов, пиктограмм, звуков, анимации.

- Все пиктограммы, присутствующие на рабочих экранах, должны в обязательном порядке быть снабжены надписями, поясняющими их назначение и разворачивающимися на экране при установке курсора в центр пиктограммы. Графическое отображение пиктограмм должны быть интуитивно понятными и нести в себе информацию о том, что это такое и что произойдет, если выбрать или произвести действие над каким-то объектом. Необходимо, чтобы пользователь имел наглядное средство отображения информации на различных этапах решения задач, он должен видеть, как его действия влияют на объекты, расположенные на экране.
- Поля экранных форм Системы должны заполняться пользователями Системы преимущественно путем выбора значений из справочников. Ширина выпадающих списков должна адаптироваться к данным, длина аналогично либо до нижней границы рабочего окна системы, если весь список не помещается.
- Интерфейс Системы должен поддерживать все разрешения экранов, используемых на рабочих местах пользователей.
- Пользователи Системы должны иметь возможность осуществлять поиск в Системе на русском и английском языке, используя стандартную функциональность программного обеспечения Системы.
- Система должна обеспечивать возможность однократной авторизации (single sign-on) при переходе между различными компонентами Системы.
- Основным интерфейсом Системы для целей планирования является MS Excel. При этом должна быть обеспечена возможность удаленного доступа к функциям системы через Web-интерфейс (с поддержкой, как минимум, браузера IE версии 8 и 9). Функциональность согласования и управления статусом бюджетного процесса должна быть реализована в виде Web-интерфейса.
- При работе с отчетами должна быть предусмотрена возможность выполнения сортировки, группировки, фильтрации.
- Система должна иметь штатные средства загрузки данных из файлов MS Excel и/или из плоских файлов (CSV).
- Система должна иметь возможность экспортировать данные в Excel-формате, не требующем дальнейших преобразований типа «текст в числа», а также выгружаемые данные должны быть максимально адаптированы к последующей сортировке, фильтрации и обработке функциями типа sum if, v(h)lookup и сводными таблицами Excel.
- Помимо преднастроенных отчётов необходим конструктор для составления произвольных отчетов с возможностью их сохранения. Произвольные отчеты могут быть созданы ключевым пользователем системы и не должны требовать привлечения разработчиков.

9. Требования к Исполнителю

- Исполнитель должен иметь действующий статус партнера SAP PCoE и предоставить в тендерной заявке копию сертификата, подтверждающего наличие действующего сертификата SAP PCoE.

Приложение

Қосымша 1 к ТЕ (тариф)260826.docx
Қосымша 3 к ТЕ (Біліктілік талаптары).docx
Приложение 3 к ТС (квалификационные требования).docx
Приложение 2 к ТС (перечень задач).docx
Қосымша 2 к ТЕ (тапсырмалар тізімі)26082026.docx
Приложение 1 к ТС (тариф).docx

Подписал Шумаков Алибек Бейбитович

Дата подписания 21.10.2026