VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS PRIVALOMOJO SVEIKATOS DRAUDIMO INFORMACINĖS SISTEMOS (SVEIDRA) MODERNIZAVIMO PASLAUGŲ PIRKIMAS

TECHNINĖ SPECIFIKACIJA

1. Sąvokos ir trumpiniai

1 lentelė. Sąvokos ir akronimai

Sutrumpinimas	Paaiškinimas
ASP	Užklausų apdorojimo programa
BPMN	Angl. Business Process Model and Notation
CLI	Angl. Command Line Interface
CSV	Failų formatas, skirtas saugoti duomenis lentelėje
DANAVIP	SVEIDROS duomenų analizės ir visuomenės informavimo posistemė
DB	Duomenų bazė
DBVS	Duomenų bazių valdymo sistema
DMA	Daugiamodulinė aplikacija
DPSDR	Draudžiamųjų privalomuoju sveikatos draudimu registras
DVS	Dokumentų valdymo sistema
EDMIS	Europos Sąjungos duomenų mainų informacinė sistema
ES/EEE	Europos Sąjunga ir Ekonominės erdvės šalys
ESDK	SVEIDRA IS Europos sveikatos draudimo kortelės išdavimo apskaitos ir kontrolės posistemė
EVIS	Eilių valdymo informacinė sistema
FVAIS	Finansų valdymo ir apskaitos informacine sistema
GĮ	Gydymo įstaiga
IP	Interneto protokolas
IS	Informacinė sistema
YAML	Duomenų serializavimo kalba
JDBC	Angl. Java Database Connectivity
JSON	Angl. JavaScript Object Notation
MDX	Angl. Multidimensional Expressions
METAS	SVEIDRA IS specialistų kvalifikacijos tobulinimo posistemė
MVC	Angl. Model View Controller
NAT IS	Naudotojų aptarnavimo tarnybos informacinė sistema
OData	Angl. Open Data Protocol
ODBC	Angl. Open Database Connectivity

Sutrumpinimas	Paaiškinimas
ODBO	Angl. Object Linking and Embedding Database for Online Analytical Processing
PASPĮ	Pirminės asmens sveikatos priežiūros įstaiga
PDVS	Pakopinis duomenų valdymas ir saugojimas
REST	Angl. Representational State Transfer
SAML	Angl. Security Assertion Markup Language
Service Desk	IT pagalbos tarnyba
SFTP	Angl. Secure File Transfer Protocol
SLA	Angl. Service Level Agreement
SOAP	Angl. Simple Object Access Protocol
SSL	Angl. Secure Socket Layer
SVEIDRA	Privalomojo sveikatos draudimo informacinė sistema
TLK	Teritorinė ligonių kasa
UML	Angl. Unified Modelling Language
VLK	Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos
VPN	Virtualus privatus tinklas
XSS	Angl. Cross Site Scripting

2. Dabartinė būsena

Privalomojo sveikatos draudimo informacinė sistema SVEIDRA pradėjo veikti 1997 m. spalio 1 d.. SVEIDRA nuostatai: https://www.e-tar.lt/portal/lt/legalAct/389e11e09cc211e58fd1fc0b9bba68a7 ; duomenų saugos nuostatai: https://www.e-tar.lt/portal/legalAct.html?documentId=c2b32a80ec9911e3bb22becb572235f5 ; techninė specifikacija: http://registrai.lt/management/object_files/get_object_file/10820/3/1361 .

SVEIDROS esamą funkcinę struktūrą sudaro:

- ESDK išdavimo ir apskaitos posistemė. Jos paskirtis:
  - registruoti ESDK pažymėjimų išdavimą;
  - tvarkyti ESDK ir jų apskaitos duomenis;
  - užtikrinti ESDK ir jų blankų kontrolę;
  - formuoti statistines ir analitines ataskaitas.
- Asmens prisirašymo prie ASPĮ kontrolės posistemė. Jos funkcijos:
  - tikrinti, ar asmuo įregistruotas ASPĮ mokant už jam suteiktas šioje ASPĮ asmens sveikatos priežiūros paslaugas;
  - tikrinti, ar asmuo neįregistruotas tuo pačiu metu kitoje ASPĮ.
- Kompensuojamų vaistų apskaitos posistemė KVAP. Jos funkcijos:
  - registruoti kompensuojamųjų vaistų ir medicinos pagalbos priemonių receptus;
  - tvarkyti vaistų ir medicinos paslaugų priemonių įsigijimo administravimo duomenis bei vykdyti kompensacijų už vaistų ir medicinos paslaugų priemonių įsigijimą apskaitą;
  - užtikrinti kompensuojamųjų vaistų ir medicinos pagalbos priemonių receptų bei jų blankų kontrolę;
  - formuoti statistines ir analitines ataskaitas.

- KVP bei asmens sveikatos priežiūros specialistų tapatybę patvirtinančių lipdukų paskirstymo ir apskaitos posistemė. Jos funkcijos:
    - registruoti kompensuojamųjų vaistų pasus bei asmens sveikatos priežiūros specialisto tapatybę patvirtinančius lipdukus;
    - tvarkyti KVP išdavimo ir asmens sveikatos priežiūros specialisto tapatybę patvirtinančių lipdukų paskirstymo duomenis bei vykdyti jų apskaitą;
    - užtikrinti KVP bei asmens sveikatos priežiūros specialisto lipdukų kontrolę;
    - formuoti statistines ir analitines ataskaitas.
- Asmens sveikatos priežiūros, odontologijos praktikos ir farmacijos specialistų (toliau – specialistų) bei spaudų, asmens sveikatos priežiūros, odontologinės priežiūros (pagalbos) įstaigų ir vaistinių (toliau – įstaigų) licencijų administravimo bei apskaitos posistemė METAS. Jos funkcijos:
    - administruoti SVEIDROS naudotojus;
    - registruoti įstaigų licencijų duomenis;
    - registruoti specialistų profesijas, profesines kvalifikacijas, išduotų licencijų ir spaudų duomenis;
    - registruoti specialistų įdarbinimus įstaigose ir tobulinimosi proceso duomenis;
    - tvarkyti asmens specialistų profesinės veiklos įskaitą ir su ja susijusius duomenis;
    - administruoti specialistų tobulinimui skiriamas lėšas, užtikrinti jų naudojimo kontrolę;
    - administruoti specialistų tobulinimosi programas ir tobulinimosi įvykius;
    - formuoti statistines ir analitines ataskaitas.
- Asmenims suteiktų stacionarinių paslaugų, kompensuojamų iš PSDF biudžeto, apskaitos posistemė SPAP. Jos funkcijos:
    - registruoti asmenims II ir III lygio stacionarinės pagalbos, slaugos ir palaikomojo gydymo, sanatorinio kurortinio gydymo, greitosios medicinos pagalbos paslaugas;
    - vykdyti asmens sveikatos priežiūros paslaugų apskaitą ir tvarkyti su ja susijusius duomenis;
    - tvarkyti asmens sveikatos priežiūros paslaugų kainas, formuoti gydymo įstaigoms sąskaitas už suteiktas sveikatos priežiūros paslaugas;
    - administruoti asmens sveikatos priežiūros paslaugoms PSDF skirtas lėšas, užtikrinti jų panaudojimo kontrolę;
    - formuoti statistines ir analitines ataskaitas.
- Asmenims suteiktų ambulatorinių paslaugų, kompensuojamų iš PSDF biudžeto, apskaitos posistemė APAP. Jos funkcijos:
    - registruoti asmenims suteiktas pirminės sveikatos priežiūros, II ir III lygio ambulatorinės konsultacinės pagalbos paslaugas;
    - vykdyti asmens sveikatos priežiūros paslaugų apskaitą ir tvarkyti su ja susijusius duomenis;
    - tvarkyti asmens sveikatos priežiūros paslaugų kainas, formuoti gydymo įstaigoms sąskaitas už suteiktas sveikatos priežiūros paslaugas;
    - administruoti asmens sveikatos priežiūros paslaugoms PSDF skirtas lėšas, užtikrinti jų panaudojimo kontrolę;
    - formuoti statistines ir analitines ataskaitas.
- Medicininės reabilitacijos ir sanatorinio (antirecidyvinio) gydymo administravimo posistemė RSAP. Jos funkcijos:
    - registruoti medicininės reabilitacijos ir sanatorinio (antirecidyvinio) gydymo paslaugas;

    - vykdyti medicininės reabilitacijos ir sanatorinio (antirecidyvinio) gydymo paslaugų apskaitą ir tvarkyti su ja susijusius duomenis;
    - tvarkyti medicininės reabilitacijos ir sanatorinio (antirecidyvinio) gydymo paslaugų kainas, formuoti gydymo įstaigoms sąskaitas už suteiktas sveikatos priežiūros paslaugas;
    - administruoti medicininės reabilitacijos ir sanatorinio (antirecidyvinio) gydymo paslaugoms PSDF skirtas lėšas, užtikrinti jų panaudojimo kontrolę;
    - formuoti statistines ir analitines ataskaitas.
- Prisirašymo prie pirminės sveikatos priežiūros įstaigų posistemė PRAP. Jos funkcijos:
    - registruoti draudžiamuosius prie pirminės asmens sveikatos įstaigos ir psichikos sveikatos centro;
    - iš registruoti draudžiamuosius iš pirminės asmens sveikatos įstaigos ir psichikos sveikatos centro;
    - administruoti ambulatorinių paslaugų PSDF skirtas lėšas, užtikrinti jų panaudojimo kontrolę;
    - formuoti statistines ir analitines ataskaitas.
- Informacijos teikimo valstybės institucijoms posistemė INVS. Jos funkcijos:
    - registruoti valstybės institucijų užklausas;
    - formuoti ataskaitas pagal valstybės institucijų užklausas;
- SVEIDROS administravimo ir SVEIDROS naudotojų apskaitos posistemė. Jos funkcijos:
    - registruoti (išregistruoti) SVEIDROS naudotojus;
    - suteikti ir tvarkyti SVEIDROS naudotojams suteiktas duomenų prieigos teises;
    - registruoti SVEIDROS naudotojų vykdytas užklausas;
    - tvarkyti SVEIDROS klasifikatorius ir žinynus;
    - užtikrinti SVEIDROS naudotojų teisių valdymą, SVEIDROS duomenų saugą;
    - formuoti statistines ir analitines ataskaitas.
- Duomenų analizės ir visuomenės informavimo posistemė (DANAVIP). Jos funkcijos:
    - peržiūrėti, spausdinti, eksportuoti į kitus formatus saugykloje kaupiamus duomenis;
    - vykdyti duomenų analizę pagal iš anksto nustatytus rodiklius;
    - vykdyti duomenų analizę įvairiais pjūviais, naudojant programines analizės priemones;
    - formuoti analitines bei statistines ataskaitas;
    - teikti viešą statistinę informaciją visuomenei.
- Viešųjų elektroninių paslaugų asmenims teikimo posistemė. Jos funkcijos:
    - sudaryti galimybę asmeniui per internetą gauti duomenis apie jam ASPĮ suteiktas paslaugas ir paslaugų kainas;
    - sudaryti galimybę asmeniui per internetą gauti duomenis apie jam išrašytus kompensuojamuosius vaistus ir jų kainas.

Planuojama šias posistemes iškelti iš SVEIDRA IS ir perkelti į kitas informacines sistemas:

1. Ortopedijos techninių priemonių paskirstymo ir apskaitos posistemė
2. Duomenų analizės ir visuomenės informavimo posistemė (toliau – DANAVIP)

Sistema automatiniu būdu duomenis gauna iš:

- Draudžiamųjų privalomuoju sveikatos draudimu registro;

- Vaistinių;
- Asmens sveikatos priežiūros įstaigų;
- Ortopedijos technikos įmonių, sudariusių sutartis su VLK dėl ortopedijos technikos gaminių tiekimo;
- optikos įmonių, sudariusių sutartis su TLK;
- ESPBI IS

Sistema automatiniu būdu duomenis teikia:

- EVIS
- EDMIS

Įstaigos ir/ar įmonės į IS SVEIDRA informaciją pateikia per tinklinių paslaugų integracinę sąsają arba prisijungdami tiesiogiai prie IS SVEIDRA naudotojo sąsajos ir suvedant informaciją tiesiogiai. Iš ESPBI IS SVEIDRA duomenis gauna naudojantis tiesiogine duomenų bazių sąsaja ir žiniatinklio paslaugomis.

Valstybinėje ligonių kasoje yra centrinė duomenų saugykla, joje tvarkoma visa sistemos duomenų bazė, atliekamas klasifikatorių ir registrų tvarkymas, duomenų apsikeitimas su kitomis įstaigomis ir/ar įmonėmis. Duomenų apsikeitimas užtikrinamas, priklausomai nuo įstaigos ir/ar įmonės, su kuria vykdomas duomenų apsikeitimas, kompiuterizuotos informacinės sistemos išsivystymo lygio ir turimų komunikacijų priemonių.

Su kiekviena įstaiga ir/ar įmone, kurios duomenys importuojami, yra pasirašyta duomenų apsikeitimo sutartis, kurioje nustatoma duomenų apsikeitimo formatai, periodiškumas, techninės priemonės, klaidų šalinimas ir pan.

Be centrinės duomenų bazės nacionaliniame lygmenyje dar yra aplikacijų serveris ir Web aplikacijoms skirta duomenų bazė. Web aplikacijoms naudojama duomenų bazė (toliau – KVP) turi ryšį su centrine duomenų baze. Centrinė duomenų bazė Oracle priemonėmis pasiima ir padeda duomenis į KVP duomenų bazę. KVP duomenų bazė tinklo atžvilgiu yra demilitarizuotoje zonoje.

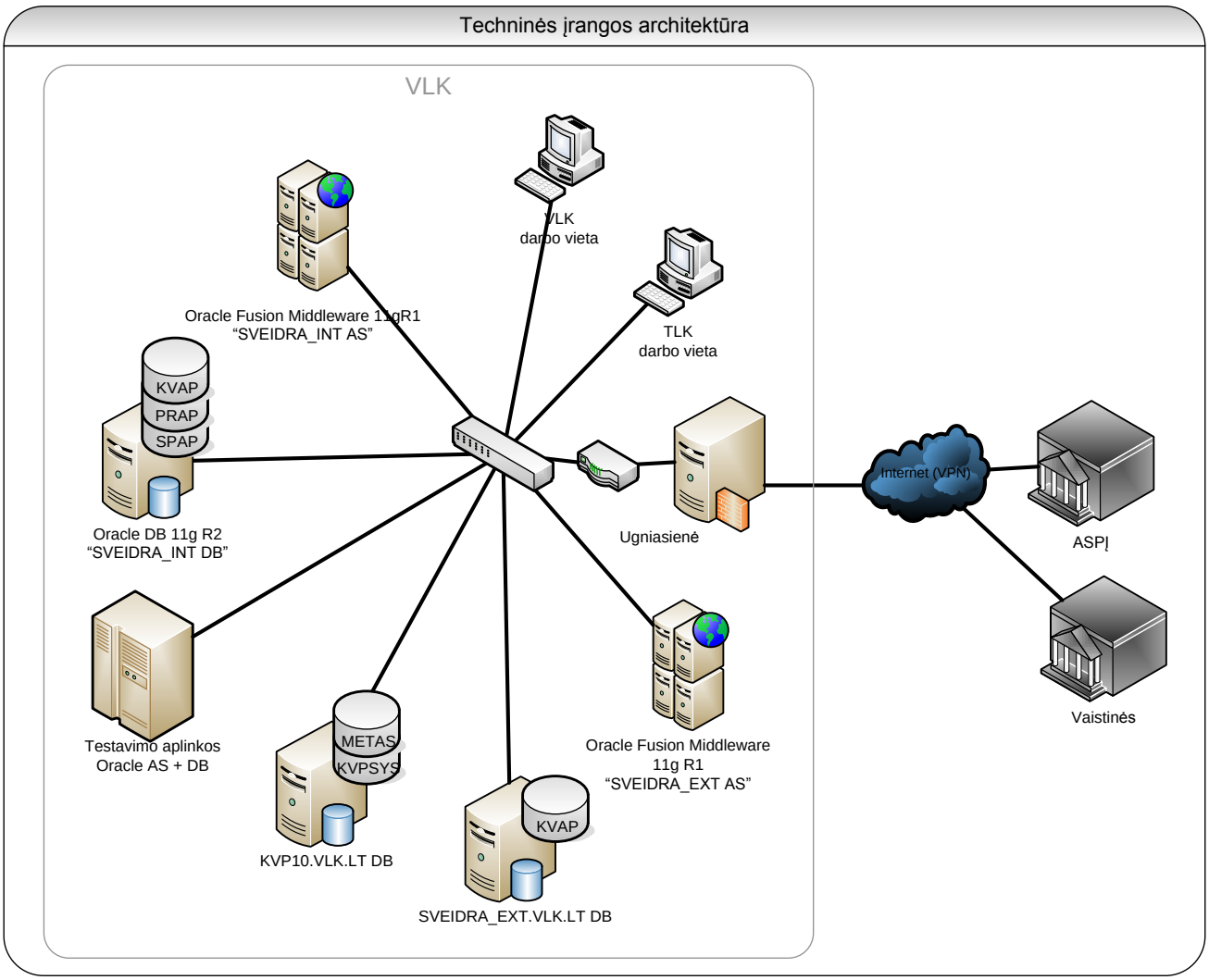
Sistemą sudaro Centrinis duomenų bazės serveris, duomenų bazės, skirtos komunikavimui su išoriniais vartotojais serveris, aplikacijų serveris, integracinis serveris, skirtas duomenų apsikeitimui su išorės institucijomis.

Iš esmės sistemą SVEIDRA galima skaidyti į dvi dalis – pirmoji veikianti web technologijų pagrindu, antroji sukurta Oracle technologijų pagrindu. Gydymo įstaigos naudojasi ir web technologijų pagrindu ir Oracle technologijų pagrindu sukurtomis SVEIDRA posistemėmis. Draustumo informaciją gydymo įstaigos tikrina per web aplikacijas arba tinklo paslaugų (angl. – web service) pagalba (duomenys gaunami iš Draudžiamųjų privalomuoju sveikatos draudimo registro, kurio valdytoja yra VLK). Informaciją apie gydymo įstaigose suteiktas paslaugas gydymo įstaigos pateikia iš gydymo įstaigose įsidiegtų ligoninių informacinių sistemų per tinklinę sąsają (angl. web servisais) arba tiesiogiai įrašydami duomenis į Oracle technologijų pagrindu sukurtas SVEIDROS posistemes pasirinktinai. Ortopedijos įmonės prie SVEIDROS ortopedijos posistemės jungiasi tik per web aplikacijas arba tinklo paslaugų pagalba. SVEIDROS posistemė, skirta endoprotezų kompensavimo duomenims apdoroti, šiuo metu nėra naudojama.

SVEIDROS naudotojai skirstomi į grupes pagal jiems priskirtas teises. Priklausomai nuo sistemoje suteiktų teisių ir poreikio naudotojai gali su sistema dirbti skirtingose sąsajose. Prie centrinės duomenų bazės per Oracle priemonėmis sukurtą sąsają leidžiama jungtis tik iš vidinio VLK tinklo per VPN prieigą. TLK yra darbuotojų, kurių darbo vieta yra ne TLK patalpose (savivaldybėje, didesnėje gydymo įstaigoje ir pan.), leidžiama jungtis tik naudojant VPN sujungimus.

Sistema naudojasi virš 10.000 naudotojų, vienu metu sistema naudoja apie 2500 naudotojų. Mobilios darbo vietos nėra naudojamos. Sistemos licencija neriboja vartotojų skaičiaus.

2.1. Pagrindiniai techninės architektūros elementai



1 paveikslas. Techninė architektūra

2 lentelė. Architektūros elementų aprašymas

Elementas	Aprašymas
Oracle Fusion Middleware 11gR1 aplikacijų serveris „SVEIDRA_INT AS“	Keturios fizinės tarnybinės stotys, kuriose sudiegta Oracle WebLogic aplikacijų serverio sisteminė programinė įranga, susidedančios iš apkrovos balansavimo serverio ir trijų aplikacijų serverių kuriuose diegiama IS SVEIDRA vidinių aplikacijų klientinė programinė įranga. Serveriai skirti vykdyti ir aptarnauti IS SVEDRA vidines aplikacijas (pasiekiamas per VPN ar VLK vidinį tinklą - SPAP, PRAP, vidinė KVAP ir kt.), kurių naudotojai ASPĮ, VLK ir TLK darbuotojai. Sąlyginai pavadintas „SVEIDRA_INT AS“ nuo angl. internal – vidinis AS.
Oracle DB 11gR2 „SVEIDRA_INT DB“	Tarnybinė stotis, kurioje įdiegta Oracle 11gR2 RAC SE duomenų bazė vidinių aplikacijų duomenų struktūroms bei duomenims saugoti. Sąlyginai pavadinta „SVEIDRA_INT DB“ nuo angl. internal – vidinė DB.
VLK darbo vieta	VLK darbo vieta darbui su klientine aplikacijų dalimi
TLK darbo vieta	TLK darbo vieta darbui su klientine aplikacijų dalimi
ASPĮ	ASPĮ darbo vieta darbui su kliento aplikacijų dalimi ir/ar ASPĮ IS darbui su tinklinių paslaugų (WS) dalimi.
Vaistinės	Vaistinės darbo vieta darbui su klientine aplikacijų dalimi ir/ar Vaistinės IS darbui su tinklinių paslaugų (WS) dalimi.
Testavimo aplinkos Oracle AS + DB	Testavimo aplinkos tarnybinės stotys.
Principinėje techninės įrangos architektūros diagramoje žymima kaip „KVP10.VLK_LT DB“ ir	Fizinė VLK turima Oracle 10.2.0.4 versijos duomenų bazės mašina, esanti demilitarizuotoje [1]zonoje. Naudojama IS Sveidra vartotojų autorizavimui, bei kitų reikalingų IS SVEIDRA aplikacijoms duomenų (gydymo įstaigos, gydytojų duom., asmenų, jų draustumo, vartotojų

[1] Iš duomenų bazės kreipiniai į vidinį VLK tinklą nėra leidžiami.

Elementas	Aprašymas
„SVEIDRA_EXT.VLK_LT DB“	prisijungimo, teisių ir rolių duomenys ir pan.) kaupimui.
Oracle Fusion Middleware 11gR1 aplikacijų serveris „SVEIDRA_EXT AS“[2]	Tarnybinė stotis, kurioje įdiegta Oracle WebLogic aplikacijų serverio sisteminė programinė įranga ir kurioje yra sudiegti IS SVEIDRA išorinių aplikacijų komponentai: klientinės bei tinklinių paslaugų (webservice) . Serveris skirtas vykdyti ir aptarnauti IS SVEIDRA išorinių aplikacijų (prieinamų internetu, pvz. vaistinės) klientus bei tinklines paslaugas (webservice). Sąlyginai pavadintas „SVEIDRA_EXT AS“ nuo angl. external – išorinis AS.

Centrinė IS SVEIDRA duomenų bazė yra 11g versijos, senieji IS SVEIDRA duomenys yra saugomi 10g versijos duomenų bazėje. Duomenys saugomi diskų masyve prijungtame SAN jungtimis.

Web aplikacijų naudojama išorinė duomenų bazė, esanti demilitarizuotoje zonoje, veikia MS Windows Server 2003 Standard Edition x64 operacinėje sistemoje. Duomenys saugomi diskų masyve prijungtame SAN jungtimis.

Web aplikacijų serveriuose naudojama MS Windows Server 2008 R2 Enterprise Edition operacinė sistema.

Integraciniame serveryje, kuris yra naudojamas duomenų mainams su išorinėmis institucijomis, naudojama MS Windows Server 2008 Standard Edition x64 operacinė sistema.

Duomenų kopijavimui į juostas bei atstatymui naudojama IBM Tivoli Storage Manager 6.1 bei IBM System Storage DS Storage Manager 10.

DANAVIP posistemė realizuota SAP Business Objects BI programinės įrangos priemonėmis, SAP Sybase IQ duomenų bazėje.

ESDK posistemė realizuota JAVA programavimo įrankių priemonėmis.

Detali Privalomojo sveikatos draudimo informacinės sistemos SVEIDRA techninė specifikacija yra paskelbta valstybės registrų ir informacinių sistemų registre, adresu: http://registrai.lt/ (Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos interneto svetainėje). Visuose prie SAN (Storage Area Network) duomenų tinklo prijungtose tarnybinėse stotyse yra įdiegta *IBM* System Storage *Multipath* Subsystem Device *Driver* programinė įranga.

[2] Ryšiui su kitomis išorinėmis aplikacijomis IS Sveidra papildomai naudoja Apache TomCat ir Oracle GlassFish aplikacijų serverius.

2011 m. SAP ERP platformos pagrindu VLK buvo sukurtas Draudžiamųjų privalomuoju sveikatos draudimu registras (DPSDR), o 2013 m. baigta diegti VLK finansų valdymo ir apskaitos informacinė sistema (FVAIS). DPSDR teikia IS SVEIDRA draudžiamųjų duomenis per integracinę sąsają, o ASPĮ gauna registro informaciją apie pacientų draustumą, naudojantis interneto portalu arba perduodant informaciją į gydymo įstaigų ir vaistinių informacines sistemas tinklo paslaugų (WS) pagalba. FVAIS yra realizuotas Privalomojo sveikatos draudimo fondo administravimo įstaigų (Valstybinės ligonių kasos bei teritorinių ligonių kasų) finansų valdymo ir apskaitos funkcionalumas bei bazinis Privalomojo sveikatos draudimo fondo apskaitos funkcionalumas, suteikiantis galimybę vykdyti apskaitą pagal Viešojo sektoriaus apskaitos ir finansinės atskaitomybės standartus (VSAFAS). VLK Finansų valdymo ir apskaitos informacinės sistemos funkcionalumą numatoma išplėsti, įdiegiant detalų Privalomojo sveikatos draudimo fondo (PSDF) finansų valdymo ir apskaitos funkcionalumą, apimantį PSDF išlaidų apskaitą pagal asmenį, sutarčių valdymą bei integracinių sąsajų su SVEIDRA ir kitomis IS realizavimą.

VLK yra įdiegta IT ir IS pagalbos tarnyba, skirta pagal ITIL metodologijas automatizuoti Incidentų valdymo, Problemų valdymo, Keitimų valdymo, Konfigūracijų valdymo, Versijų valdymo ir Paslaugų lygio valdymo procesus. Įdiegus IT ir IS pagalbos tarnybą visi VLK valdomų informacinių sistemų incidentai, problemos, keitimai, konfigūracijos bei versijos yra valdomos centralizuotai, per VLK IT ir IS pagalbos tarnybą.

SVEIDRA IS veikimui užtikrinti yra naudojamos šios Oracle licencijos:

3 lentelė. SVEIDRA IS Oracle licencijos

Nr.	Licencijos pavadinimas	Licencijos tipas
1.	Oracle Database Standard Edition licencija	Processor Perpetual Full Use
2.	Oracle Database Enterprise Edition licencija	Processor Perpetual Full Use
3.	Partitioning licencija	Processor Perpetual Full Use
4.	Data Mining licencija	Processor Perpetual Full Use
5.	OLAP licencija	Processor Perpetual Full Use
6.	Spatial and Graph licencija	Processor Perpetual Full Use
7.	Oracle Internet Application Server Enterprise Edition licencija	Processor Perpetual Full Use
8.	Oracle Weblogic Suite licencija	Processor Perpetual Full Use
9.	Oracle SOA Suite for Oracle Middleware licencija	Processor Perpetual Full Use
10.	Internet Developer Suite licencija	NUP Perpetual Full Use
11.	Oracle Data Integrator Enterprise Edition licencija	Processor Perpetual Full Use
12.	Oracle Business Intelligence Suite Enterprise Edition Plus licencija	Processor Perpetual Full Use
13.	Oracle Forms and Reports licencija	Processor Perpetual Full Use
14.	Oracle Weblogic Server Standard Edition licencija	Processor Perpetual Full Use
15.	Oracle Database Enterprise Edition papildoma opcija Diagnostic Pack licencija	Processor Perpetual Full Use
16.	Oracle Database Enterprise Edition papildoma opcija Tunning Pack licencija	Processor Perpetual Full Use
17.	Oracle Advanced Security licencija	Processor Perpetual Full Use

18.	Oracle Standard Edition One licencija	NUP Perpetual Full Use

3. Siekiama būsena

Modernizuojant SVEIDRA, siekiama iš esmės supaprastinti esamą architektūrą iš techninės pusės bei optimizuoti ir pagreitinti naudotojų funkcionalumą. Taip pat siekiama stipriai sumažinti metines sistemos išlaikymo išlaidas.

Visur pasaulyje toliau eksponentiškai augant gaunamų ir apdorojamų duomenų kiekiui – esamos tradicinės duomenų saugojimo ir apdorojimo sistemos dažnai susiduria su aibe problemų – jos nėra pakankamai greitos bei pakankamai lanksčios, tačiau tradiciškai reikalauja didelių palaikymo resursų – tiek finansinių, tiek techninių ir žmogiškųjų. Tokiu būdu grąža iš tradicinių sistemų mažėja ir tai tampa vis didesne našta organizacijoms, kurios privalo saugoti ir apdoroti vis daugiau duomenų, kurti ir eksploatuoti naujas elektronines paslaugas bei tenkinti vis daugiau teisinių ir kitų reikalavimų. Žiūrint ir operatyvinės pusės – dideli išlaikymo kaštai riboja plėtros ir inovacijų galimybes.

Siekiant pakeisti susiformavusį ciklą, t.y. sumažinti išlaikymo kaštus bei sudaryti daugiau galimybių naujų funkcijų diegimui ir esamų funkcijų tobulinimui, turi būti pritaikytos moderniausios tendencijos ir technologijos.

Pagrindinis techninės architektūros supaprastinimo akcentas – apjungti transakcines ir analitines DB į vieną, panaudojant šiuo metu išpopuliarėjusias „in-memory“ technologijas, kurios leidžia visus reikalingus sistemos veikimui duomenis saugoti operatyvinėje atmintyje, tokiu būdu radikaliai pagreitinant visas duomenų apdorojimo užklausas – tiek transakcines, tiek analitines. Toks architektūros modernizavimas leis supaprastinti:

- Techninės įrangos architektūrą – nebereikės atskirų DB transakciniams ir analitiniams duomenims.
- SVEIDRA duomenų modelį, atsisakant daugelio duomenų pakrovimo ir transformavimo procedūrų.
- Atitinkamai tikimasi sumažinti ir operatyvines išlaidas – tiek techninės ir programinės įrangos licencijų priežiūros, tiek viso sprendimo priežiūros ir palaikymo.

Numatoma, kad tokiu būdu supaprastinta SVEIDRA architektūra ir struktūra žymiai pagreitins naudotojų darbą. Priklausomai nuo konkretaus scenarijaus duomenų užklausos galės būti vykdomos nuo kelių iki keliolikos kartų greičiau. Tai būtų esminė ir pati didžiausia modernizuotos SVEIDRA IS naudotojams teikiama nauda.

Kitas paprastesnio ir lankstesnio duomenų modelio ir architektūros numatomas privalumas – platesnės galimybės efektyvinti ir tobulinti esamus procesus bei diegti naujas funkcijas bei paslaugas. Iki šiol bet koks didesnis sistemos modifikavimas buvo siejamas su nemaža rizika bei kaštais. Iš tiesų dėl istorinių aplinkybių bei ilgo sistemos eksploatavimo laiko dažnai nebuvo įmanoma tiksliai įvertinti šių rizikų bei kaštų. Modernizuojant SVEIDRA, iš esmės nauja sistema taps skaidri ir lengviau valdoma,

sumažės vidinių sąsajų ir techninių komponentų skaičius. Bus atlikta pilna detali analizė, atnaujinta dokumentacija. Visa tai turi sudaryti bazę naujos kartos elektroninių paslaugų kūrimui, realaus laiko duomenų pateikimui ir analizei.

Paskutinis esminis siekiamas akcentas – mažesni eksploatavimo kaštai. Tai turėtų paliesti tiek programinės įrangos bei techninės įrangos aptarnavimo išlaidas, tiek pačios sistemos eksploatavimo kaštus. Būtų sudaryta prielaida skirti daugiau resursų paslaugų vystymui.

4. Viešojo pirkimo sutarties tikslai, uždaviniai, veiklos ir rezultatai

Projekto tikslas - modernizuoti SVEIDRA IS, sukuriant naujas ir modernizuojant esamas elektronines paslaugas, projekto vykdymo metu užtikrinant šiuo metu veikiančios SVEIDRA IS veikimą.

Uždaviniai:

- Perkelti SVEIDRA IS į vieningą technologinę platformą.
- Sumažinti SVEIDRA IS licencijų ir licencijų palaikymo kaštus.
- Sumažinti SVEIDRA IS aptarnavimo kaštus.
- Modernizuoti SVEIDRA IS duomenų bazės struktūrą (duomenų modelį) siekiant sudaryti sąlygas kurti naujas ir modernizuoti esamas funkcijas.
- Modernizuoti SVEIDRA IS išorinį ir vidinį portalą, panaudojant šiuolaikines technologijas ir geriausias praktikas.
- Modernizuoti SVEIDRA IS integracines sąsajas.
- Atnaujinti SVEIDRA IS dokumentaciją.

Diegėjas turi pasiūlyti Perkančiajai organizacijai SVEIDRA IS modernizavimo strategiją ir kiekvienos posistemės modernizavimo planą, kuris turi apimti šiuos etapus:

- Planavimas;
- Detali analizė;
- Projektavimas;
- Konstravimas;
- Testavimas;
- Mokymai;
- Diegimas;
- Duomenų migravimas;
- Bandomoji eksploatacija;
- Įvedimas į eksploataciją;
- Garantines paslaugos.

Tiekėjų siūloma SVEIDRA IS modernizavimas turi būti vykdomas vadovaujantis 2014 m. vasario 25 d. Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus įsakymu Nr. T-29

“Dėl Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtinimo” ir jame nurodytomis informacinių sistemų kūrimo metodikomis.

Tiekėjo SVEIDRA IS modernizavimo strategijai yra taikomi šie reikalavimai:

1. Pirmiausia Tiekėjas turi modernizuoti SVEIDROS administravimo ir SVEIDROS naudotojų apskaitos posistemę bei išspręsti klasifikatorių valdymo uždavinį.
2. Pirmoji SVEIDRA IS posistemė turi būti sukurtą per ne ilgesnį kaip 9 mėn. laikotarpį, neįskaitant bandomosios eksploatacijos.
3. Kitos SVEIDRA IS posistemės turi būti modernizuotos ir paleistos į bandomąją eksploataciją ne rečiau nei kas 6 mėn. Tuo atveju, kai posistemės tarpusavyje stipriai susiję veiklos procesais ir yra netikslinga kurti laikinas integracines sąsajas tarp senojoje ir naujojoje platformoje veikiančių posistemių, turės būti modernizuojamos vienu metu pradedamos eksploatuoti kelios daugiau tarpusavyje susijusios posistemės. Tiekėjas techniniame pasiūlyme turi pateikti Sveidros posistemių migravimo į vieningą technologinę platformą eiliškumą ir trukmes.
4. Kiekvienos iš posistemių bandomosios eksploatacijos trukmė negali viršyti 4 mėn.
5. Modernizavus visas sistemos posistemes bus vykdoma visos modernizuotos SVEIDRA IS bandomoji eksploatacija – iki 4 mėn.
6. Baigus sistemos bandomąją eksploatacija turi būti teikiamos 12 mėn. trukmės garantijos paslaugos.

SVEIDRA IS privalo būti modernizuota per 36 mėn. nuo sutarties pasirašymo pradžios. Po modernizuotos SVEIDRA IS įvedimo į eksploataciją turi būti teikiamos nemokamos 12 mėn. garantijos paslaugos pagal LR Civiliniame kodekse nustatytus garantijos suteikimo reikalavimus. Garantijos laikotarpio metu Tiekėjas turi taisyti atsiradusias klaidas bei funkcijų sutrikimus, atsiradusius tik dėl Tiekėjo kaltės. Garantijos apimtyje esančia klaida ar funkcijos sutrikimu yra laikomas IS atliekamų funkcijų neatitikimas (funkcijų neveikimas) techninėje specifikacijoje aprašytiems reikalavimams.

Tiekėjas turi numatyti, kad posistemės yra tarpusavyje susijusios bendrais veiklos procesais ir jose naudojami bendri klasifikatoriai, todėl sistemos migravimo į vieningą platformą metu gali būti reikalinga sukurti laikinas integracines sąsajas tarp senojoje ir naujojoje platformoje veikiančių posistemių. Tiekėjas, teikdamas pasiūlymą turi įskaityti laikinų integracinių sąsajų sukūrimo ir palaikymo kaštus.

Svarbu: Tiekėjai, siūlydami SVEIDROS IS modernizavimo paslaugas privalo vadovautis Valstybės informacinių išteklių valdymo įstatymu (2011 m. gruodžio 15 d. Nr. XI-1807), ir 2013 m. vasario 27 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 180 “Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo”, ir 2013 m. liepos 24 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 716 “Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo” ir 2014 m. vasario 25 d. Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus įsakymu Nr. T-29 “Dėl Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtinimo” bei atsižvelgti į Lietuvos Respublikos standartus LST ISO/IEC 12207:1995, LST ISO/IEC 20000-1:2015 bei LST ISO/IEC 27001 standartą.

Rezultatai:

- Pilna apimtimi modernizuotas, įdiegtas ir ištestuotas SVEIDRA IS sprendimas, įskaitant:
    - SVEIDRA IS duomenų bazės modernizavimą;
    - SVEIDRA IS aplikacijų modernizavimą;
    - Integracinių sąsajų modernizavimą;
    - Įgyvendinti visi papildomi funkciniai reikalavimai (skyrius 5.2);
    - Parengta (atnaujinta) ir patvirtinta modernizuotos SVEIDRA IS dokumentacija.
- Sumažinti SVEIDRA IS reikalingų licencijų palaikymo kaštai.

5. SVEIDRA IS modernizavimo funkciniai reikalavimai

1. Tiekėjas privalo realizuoti visus šios specifikacijos funkcinius ir nefunkcinius reikalavimus.

5.1. Bendri funkciniai reikalavimai

2. Modernizuota SVEIDRA turi išlaikyti ne žemesnį funkcionalumo lygį, negu yra šiuo metu.
3. Modernizuota SVEIDRA turi išlaikyti esamą funkcinį duomenų modelį, atsižvelgiant į žemiau išvardintus papildomo funkcionalumo reikalavimus, nefunkcinius reikalavimus bei modernizuotos sistemos suteikiamas naujas galimybes ir technologijas.
4. Modernizuota SVEIDRA turi išlaikyti esamą funkcinį naudotojo sąsajos ir ataskaitų lygį, atsižvelgiant į žemiau išvardintus papildomo funkcionalumo reikalavimus, nefunkcinius reikalavimus bei modernizuotos sistemos suteikiamas naujas galimybes ir technologijas.
5. Modernizuota SVEIDRA turi išlaikyti esamą funkcinį integracinių sąsajų lygį, atsižvelgiant į žemiau išvardintus papildomo funkcionalumo reikalavimus, nefunkcinius reikalavimus bei modernizuotos sistemos suteikiamas naujas galimybes ir technologijas.
6. Tiekėjas turi įvertinti, kad vykdomo projekto metu bus atliekami pakeitimai senojoje Sveidros versijoje, kurie taip pat turės būti perkelti į vieningą technologinę platformą.

5.2. Kiti funkciniai reikalavimai

7. Tiekėjas turi modernizuoti Kompensuojamų vaistų pasų bei asmens sveikatos priežiūros specialistų tapatybę patvirtinančių lipdukų paskirstymo ir apskaitos posistemę (KVP) užtikrinant, kad:

    - posistemė funkcionuotų vidinėje SVEIDRA aplinkoje (šiuo metu veikia išorinėje) išlaikant esamą posistemės funkcionalumą;
    - posistemė veiktų su naujausiomis interneto naršyklėmis (posistemė buvo realizuota technologijomis, kurios nėra palaikomos naujosiose interneto naršyklėse);
    - tarp KVAP ir KVP posistemių būtų tinkamas abipusis duomenų sinchronizavimas arba būtų naudojama ta pati duomenų bazė;

- kompensuojamų vaistų pasų išdavimo kainos keitimas būtų parametrizuotas ir keičiamas per naudotojo sąsają;
- veiktų per asmens sveikatos priežiūros įstaigų naudojamą saugų ryšį.
  Pastaba: Perkančiajai organizacijai būtų priimtinas KVAP ir KVP posistemių perkėlimas į vieną posistemę vieningoje technologinėje platformoje.

  Svarbu: Jeigu projekto vykdymo metu, pereinant prie elektroninio recepto, būtų atsisakyta kompensuojamųjų vaistų pasų ir asmens sveikatos priežiūros specialistų tapatybę patvirtinančių lipdukų, KVP posistemės perkėlimo gali būti atsisakyta. Vietoj šių darbų galės būti užsakyti SVEIDROS plėtros darbai.

8. SVEIDRA generuojamų ataskaitų už ilgesnį nei 1 mėnesio periodą greitaveikos optimizavimas.
9. Žiniatinklio paslaugų modifikavimas stebėjimui:

   - žiniatinklio paslaugomis teikiamos informacijos naudojimo parametrizavimas;
   - žiniatinklio paslaugų naudojimo statistikos realizavimas.

10. Standartinės programinės įrangos ir infrastruktūros modifikavimas:

    - tinklo paslaugų greitaveikos optimizavimas;
    - duomenų ir aplikacijos migravimas į naujos versijos duomenų bazių valdymo sistemą, esant poreikiui;
    - aplikacijų serverių optimizavimas;
    - automatinio parametrizuojamo duomenų iškrovimo iš žurnalinių lentelių realizavimas tam, kad būtų sumažintas duomenų bazės dydis.

11. Integracinių sąsajų modifikavimas:

    - esamų integracinių sąsajų modernizavimas;
    - duomenų teikimo mechanizmų modernizavimas.

12. Naujų integracinių sąsajų sukūrimas:

    - su Eilių valdymo informacine sistema;
    - su Europos duomenų mainų informacine sistema
    - „iDrug“ informacine sistema (kompensuojamųjų ir nekompensuojamųjų vaistinių preparatų ir kompensuojamųjų medicinos pagalbos priemonių kainų deklaravimo ir kainynų sudarymo informacinė sistema) per VIISP;
    - su Dokumentų valdymo sistema.

13. Informacijos apie teiktus asmens duomenis kaupimas ir asmenų teisės apie teiktus jų asmens duomenis tretiesiems asmenims įgyvendinimas.
14. Informacinių posistemių (pvz. METAS, ESDK, KVP) viešųjų dalių modernizavimas užtikrinant duomenų saugą, duomenis teikiant SSL arba lygiaverčiu protokolu arba panaudojant VPN ryšį.
15. METAS posistemės greitaveikos optimizavimas.
16. SVEIDRA IS funkcijų vykdymo laiko optimizavimas.

17. Analizės metu identifikuotiems posistemių objektams leisti įvesti būseną „Anuliuotas“, „Techninė klaida“ ir kt. Tokią būseną kaupti duomenų bazių lentelėse ir pagal ją atlikti atranką tam, kad nebūtų rodomi anuliuoti (neaktualūs) įrašai išoriniams naudotojams (pvz. ASPĮ darbuotojams).
18. Įgyvendinti galimybę TLK darbuotojams naudojantis formomis atstatyti anuliuotus dėl duomenų iš kitų institucijų vėlavimo kompensuojamųjų vaistų pasus, kitus TKL tvarkomus duomenis.
19. APAP posistemėje naujų taisyklių sukūrimas.
20. APAP posistemėje esamų funkcijų tobulinimas.
21. Visose SVEIDRA posistemėse sutvarkyti ryšius tarp sutarčių ir paslaugų nomenklatūros.
22. Įgyvendinti asmens paslaugų statistinių apskaitos kortelių „judėjimą“ su pacientu gydymo įstaigos lygyje (tarp padalinių) ir tarp gydymo įstaigų.
23. Įgyvendinti galimybę eksportuoti duomenis į Excel ar lygiaverčio formato bylą iš bet kokios formos. Duomenų eksportui būtinos teisės turi būti nustatytos gydymo įstaigų, TLK ir VLK lygmenyse. Pateikti eksportui į bylas duomenys turi būti žurnalizuojami, saugomas duomenų eksporto faktas ir meta duomenys apie turinį.
24. Realizuoti naudotojų veiksmų registravimo žurnale asmens duomenų skaitymo veiksmo registravimą.
25. Įgyvendinti gydytojo teikiamų paslaugų kontrolę pagal specialisto licenciją.
26. Išspręsti problemą dėl papildomo draustumo mėnesio.
27. Realizuoti reabilitacijos paslaugų kvotų mechanizmą.
28. Prisirašymo mechanizmo patikslinimas (būna, kad kūdikiai drausti, tačiau nepatenka į ataskaitą).
29. RSAP turi būti galimybė įvesti neidentifikuotą asmenį 70 formoje. (Ne Lietuvos pilietis su ESDK kortele, gaunantis būtinąsias reabilitacijos paslaugas). Pildant 070/a-LK formą neturi būti galimybės pasirinkti ne to asmens ambulatorinę kortelę ir taip pat 025/a-LK formoje turi būti galimybė pašalinti ne to asmens 070/a-LK kortelę.

6. SVEIDRA IS modernizavimo nefunkciniai reikalavimai

6.1. Reikalavimai programinei įrangai

6.1.1. Reikalavimai duomenų valdymo platformai

30. Duomenų valdymo platforma turi būti naujos kartos DBVS su galimybe visus aktyvius duomenis laikyti operatyvinėje atmintyje, siekiant žymiai greitesnio jų apdorojimo.
31. DBVS turi greitai apdoroti visas transakcines ir analitines užklausas naudojant vieną duomenų kopiją, t.y. sistema turi sugebėti teikti ir apdoroti ataskaitas bei kitus analitinius objektus naudojant transakcinius duomenis realiu laiku.
32. Platforma turi leisti saugoti duomenis skirtingų tipų duomenų lentelėse: stulpelinio tipo, eilučių tipo, nenustatyto tipo.
33. Platforma turi leisti nustatyti duomenų lentelių saugojimo parametrą – diską arba operatyvinę atmintį.
34. DBVS turi palaikyti šiuos atvirus duomenų mainų standartus – REST, JSON, ODBO, MDX, ODBC ir JDBC arba lygiaverčius.
35. DBVS turi turėti galimybę rečiau naudojamus duomenis saugoti ir apdoroti diske, o ne atmintyje.
36. Platforma turi sugebėti pradėti aptarnauti užklausas iškart po paleidimo bei atvirkščiai pirmiausia sulaukti visų duomenų pakrovimo į atmintį.
37. DBVS turi turėti standartinį pakopinio duomenų valdymo ir saugojimo (toliau – PDVS) funkcionalumą, kuris leistų valdyti duomenis priklausomai nuo jų naudojamo dažnumo ir kitų parametrų bei kilnoti tarp duomenų saugojimo laikmenų (pvz. iš operatyvinės atminties į SAN .

38. PDVS modulis turi būti integruojamas su trečiųjų šalių rezervinio kopijavimo programine įranga.
39. PDVS modulis turi palaikyti aukšto prieinamumo konfigūravimą.
40. PDVS modulis turi turėti statistikos kaupimo galimybę, kuri yra naudojama optimizuojant užklausas. Turi būti galimybė rinkti statistiką visai lentelei arba konkretiems stulpeliams.
41. PDVS modulis turi turėti integruotus stebėjimo įrankius, kurie turi leisti stebėti pagrindinius techninius rodiklius – atmintį, disko vietą, servisų būsenas, aktyvias/pasyvias sesijas ir t.t.
42. DBVS turi turėti rolėmis pagrįstą (angl. Role-based) naudotojų teisių mechanizmą - turi būti galimybė panaudoti standartines bei kurti naujas roles ir priskirti jas naudotojams.

6.1.2. Reikalavimai integracinei platformai

43. Modernizuota SVEIDRA turi naudoti vieną iš dabar VLK naudojamų integracinių terpių: Oracle SOA Suite arba SAP Process Integration.
44. Tiekėjas siūlydamas naudoti kitą integracinę terpę, privalės pateikti jos naudojimui reikalingas programinės įrangos licencijas, o pati integracinė terpė turi atitikti žemiau esančius reikalavimus:
    - 44.1. Būti centralizuota integracine platforme – integruotą veikimo terpę ir įrankius sąsajoms tarp sistemų ir tarp modulių kurti ir valdyti.
    - 44.2. Integracinė platforma turi turėti integracinių sąsajų, veiklos procesų ir veiklos taisyklių funkcionalumą.
    - 44.3. Veiklos procesų funkcionalumas turi suteikti galimybes modeliuoti, sujungti, testuoti, diegti bei stebėti ir palaikyti sudėtingus veiklos procesus.
    - 44.4. Veiklos taisyklių funkcionalumas turi suteikti galimybę modeliuoti, konfigūruoti, diegti, vykdyti bei stebėti kompleksines veiklos taisykles, kurių tikslas – automatizuoti sprendimų priėmimą.
    - 44.5. Integracinė platforma turi palaikyti naujausią standartizuotą techninį procesų aprašo formatą – BPMN 2.0 arba lygiavertį.
    - 44.6. Procesų aprašo formatas turi leisti pilnai aprašyti diegiamo proceso komponentus – visas veiklas bei užduotis, metaduomenis, roles bei kitus parametrus.
    - 44.7. Integracinė platforma turi palaikyti mažiausiai šiuos duomenų mainų protokolus bei mechanizmus – REST, SOAP, SFTP, OData, IDoc, JDBC, el. pašto (SMTP, IMAP, POPSMTP, IMAP, POP3) arba lygiaverčius.
    - 44.8. Integracinė platforma turi turėti standartinius vidinius komponentus, sugebančius transformuoti pranešimus iš vieno aukščiau išvardinto formato į kitą.
    - 44.9. Integracinė platforma turi turėti standartinius vidinius pranešimų formavimo komponentus, sugebančius duomenis iš vienos pranešimo struktūros perkelti į kitą.
    - 44.10. Integracinė platforma turi turėti standartinį vidinį pranešimų adresavimo funkcionalumą, kuris leistų konfigūruoti įvairius pranešimų perdavimo scenarijus priklausomai nuo integracinių taisyklių ir paties pranešimo duomenų.
    - 44.11. Integracinė platforma turi turėti modeliavimo įrankius, kuriais Perkančiosios Organizacijos veiklos ekspertai galėtų be techninių žinių valdyti veiklos procesų modelių aprašus.
    - 44.12. Integracinė platforma turi turėti standartines priemones, leidžiančias pagal veiklos ir integracinių procesų aprašus generuoti naudotojo sąsajos komponentus.
    - 44.13. Integracinė platforma turi turėti standartinį komponentą visoms naudotojo užduotims valdyti. Komponentas turi leisti:

- Grupuoti, rūšiuoti bei filtruoti naudotojo užduotis, atlikti jų paiešką;
- Peržiūrėti užduočių išsamią informaciją – standartinius bei nestandartinius atributus;
- Atlikti proceso modelio nustatytus veiksmus su užduotimis. Turi būti galimybė masiniu būdu atlikti tą patį veiksmą;
- Komentuoti užduotis, prikabinti failus ir t.t.

44.14. Integracinė platforma turi turėti standartinius komponentus sąsajoms su Perkančiosios Organizacijos naudojamomis informacinėmis sistemomis kurti.

44.15. Integracinė platforma turi turėti standartines galimybes fiksuoti proceso vykdymo metu kylančius įvykius bei informuoti prisiregistravusius komponentus. Įvykių registravimo/generavimo funkcionalumas turi būti paremtas plačiai naudojamu ir lengvai integruojamu standartu (pvz. Java Message Service arba lygiaverčiu).

44.16. Integracinė platforma turi leisti atskirai valdyti integracinių komponentų funkcinius elementus bei konfigūracijos elementus, taip pat turi leisti atskirai juos perkelti iš vienos aplinkos į kitą.

6.1.3. Reikalavimai aplikacijų platformai

45. Siūlomo sprendimo aplikacijų platforma turi turėti plačias bei lanksčias aplikacijų vystymo ir konstravimo galimybes.
46. Aplikacijų platforma turi būti pilnai integruota su DBVS platforma tokiu būdu, kad visos operacijos būtų atliekamos kuo arčiau duomenų lygmens (vertinant iš trijų sluoksnių architektūros prizmės).
47. Aplikacijų platforma turi turėti tiek grafines taip ir komandinės eilutės priemones.
48. Aplikacijų platforma turi turėti šiuos komandinės eilutės įrankius:

- Aplikacijų valdymo;
- Paslaugų valdymo;
- Naudotojų, organizacijų bei erdvių valdymo;
- Valdymo ir konfigūravimo;
- Priedų valdymo;
- Aplinkų valdymo;
- Saugumo.

49. Aplikacijų platforma turi turėti standartines priemones autorizacijų ir rolių hierarchijai sukurti panaudojant statinius (apibrėžtus konstravimo metu) bei dinaminius (apibrėžtus konstravimo metu bet priklausančius nuo operacijos konteksto) parametrus.
50. Aplikacijų platforma turi palaikyti standartinius nepriklausomus autentikacijos ir autorizacijos servisus kiekvienai atskirai aplikacijai.
51. Aplikacijų platforma turi turėti standartinį užklausų maršrutizavimo modulį, kuris turi užtikrinti užklausų perdavimą atitinkamiems aplikacijų servisams užtikrinant prieigos saugumą.
52. Aplikacijų platforma turi turėti standartinius aplikacijų gyvavimo ciklo ir stebėsenos valdymo modulius.
53. Aplikacijų platforma turi palaikyti šiuos naudotojų tipus:

- Aplikacijų naudotojai – naudotojai, turintys teisę naudoti konkrečias platformoje įdiegtas aplikacijas.
- Konstravimo naudotojai (programuotojai) – naudotojai, turintys teisę konstruoti, diegti ir palaikyti aplikacijas.
- Administratoriai – naudotojai, turintys teisę keisti platformos konfigūraciją.

54. Aplikacijų platforma turi leisti kurti duomenų modelį (transakcijų ir analitinį) bei visus susijusius duomenų apdorojimo procedūras, funkcijas bei kitus komponentus.
55. Aplikacijų platforma turi turėti duomenų valdymo komponentų konstravimo priemones, kurios būtų naudojamos duomenų skaitymo/rašymo operacijoms pagal funkcinius reikalavimus aprašymui ir konstravimui bei šių operacijų suteikimui naudotojų aplikacijoms.
56. Aplikacijų platforma turi turėti naudotojo sąsajos komponentų konstravimo priemones.
57. Aplikacijų platforma turi turėti navigacijos tarp naudotojo sąsajos komponentų konstravimo priemones.

6.1.4. Reikalavimai valdymo įrankiams

58. Siūlomas sprendimas turi turėti šių tipų valdymo įrankius (arba lygiaverčius):

- Darbastalio priemones (Desktop-based), kurios leidžia atlikti visus stebėjimo ir valdymo veiksmus greitoje ir patogioje aplinkoje IT specialisto kompiuteryje.
- Internetines priemones (Web-based), kurios leidžia labai greitai atlikti daugelį stebėjimo ir valdymo veiksmų, naudojant interneto naršyklę.
- Komandinės eilutės (CLI – angl. Command line interface) įrankiai, kurie leidžia atlikti visus stebėjimo ir valdymo veiksmus bei suteikia daugiausia galimybių automatizuoti užduotis, generuoti ataskaitas ir pan.

59. Įrankiai turi turėti standartinį pakeitimų perkėlimo funkcionalumą, kuris turi leisti sprendimo artefaktus perkelti iš vienos sistemos aplinkos į kitą (pvz. iš testavimo aplinko į gamybinę aplinką).
60. Valdymo įrankiai turi būti integruoti į bendrą saugumo architektūrą, t.y. rolių pagrindu leisti arba neleisti naudotojams dirbti su tam tikru funkcionalumu. Turi būti galima naudoti kaip standartines, taip ir nestandartines roles.
61. Valdymo įrankiai turi turėti standartines sistemos administravimo priemones – turi būti standartinės funkcijos visų sistemos duomenų bazių ir įvykių valdymui.
62. Valdymo įrankiai turi turėti standartines duomenų bazių administravimo priemones – turi būti standartinės funkcijos procesų ir paslaugų valdymui, techninių resursų (atminties, procesorių, diskų ir t.t.) valdymui, sisteminių įvykių stebėjimui.
63. Valdymo įrankiai turi turėti standartines rezervinio kopijavimo, duomenų replikavimo, atstatymo valdymo priemones – turi būti standartinės funkcijos stebėsenai, rezervinių kopijų grafiko valdymui, sistemų replikavimo nustatymo peržiūrai ir valdymui.
64. Valdymo įrankiai turi turėti standartines greitaveikos stebėsenos ir valdymo priemones – turi būti standartinės funkcijos apkrovos stebėsenai, įrašymui, atkartojimui ir analizei.
65. Valdymo įrankiai turi turėti standartines bendro sistemos saugumo valdymo priemones – turi būti standartinės funkcijos tinklo saugumo, žurnalizavimo, saugyklos saugumo ir autentifikavimo valdymui.

66. Valdymo įrankiai turi turėti standartines naudotojų valdymo priemones – turi būti standartinės funkcijos naudotojų priskyrimui rolės bei rolių priskyrimui resursų (funkcijų) grupėms sistemoje.
67. Valdymo įrankiai turi turėti standartines sertifikatų valdymo priemones – turi būti standartinės funkcijos sertifikatų saugyklos ir kolekcijų valdymui.
68. Valdymo įrankiai turi turėti standartines gyvavimo ciklo valdymo funkcijas:

    - Sistemos ir atskirų jos komponentų (standartinių ir papildomų) diegimo ir atnaujinimo priemonės.
    - Sistemos architektūros valdymo priemonės, įskaitant sistemos struktūrinės informacijos perdavimas ir registravimas centrinėje sistemų valdymo duomenų bazėje.
    - Valdyti sistemos serverių roles, pridėti ir naikinti serverius ir jų roles.

69. Valdymo įrankiai turi turėti standartines procesų stebėsenos ir valdymo funkcijas:

    - Bendras procesų vykdymo aplinkos stebėjimo priemones.
    - Įdiegtų procesų komponentų valdymo priemones su galimybe inicijuoti naują procesą.
    - Inicijuotų procesų vykdymo stebėjimo ir kontrolės priemones.
    - Inicijuotų procesų užduočių vykdymo stebėjimo ir kontrolės priemones.
    - Procesų vykdymo audito įrašų peržiūros ir analizės priemones.
    - Procesų vykdymo problemų identifikavimo ir analizės priemones.
    - Procesų duomenų archyvavimo priemones.

70. Valdymo įrankiai turi turėti standartines taisyklių stebėsenos ir valdymo funkcijas:

    - Įkelti, redaguoti bei šalinti taisyklių artefaktus nestabdant vykdymo komponentų.
    - Prieigos valdymo priemones, kurios turi užtikrinti, jog tik tam atitinkančias roles turintys naudotojai galėtų atlikti taisyklių valdymo veiksmus.
    - Taisyklių redagavimo priemones.
    - Taisyklių artefaktų versijų kontrolės priemones.
    - Taisyklių vykdymo ataskaitų generavimo priemones.
    - Taisyklių diegimo nestabdant sistemos priemones.

71. Valdymo įrankiai turi turėti standartines integracinių sąsajų stebėsenos funkcijas:

    - Peržiūrėti sąsajos detales – komponentų versijas, pavadinimus ir t.t.
    - Stebėti pranešimų kiekius pagal skirtingas būsenas.
    - Peržiūrėti pranešimų detales – laiko žymas, turinį, atributus.

72. Valdymo įrankiai turi turėti standartines integracinių sąsajų darbų sekų stebėsenos ir valdymo funkcijas:

    - Peržiūrėti sekos detales;
    - Peržiūrėti sekos gautų ir išsiųstų pranešimų kiekį bei informaciją;
    - Stabdyti/startuoti seką, esant klaidingai situacijai;
    - Nutraukti seką, esant klaidingai situacijai;
    - Peržiūrėti ir valdyti sekos žingsnius ir visą su jais susijusią informaciją.

73. Sprendimas turi leisti atlikti stebėjimo ir administravimo darbus naudojant centralizuotą Perkančiosios Organizacijos sistemų valdymo įrankį.

6.1.5. Reikalavimai vystymo/konstravimo įrankiams

74. Siūlomas sprendimas turi turėti šių tipų vystymo/konstravimo įrankius:

    - Darbastalio priemones (Desktop-based), kurios leidžia atlikti visus kūrimo ir konfigūravimo veiksmus greitoje ir patogioje aplinkoje IT specialisto kompiuteryje.
    - Internetines priemones (Web-based), kurios leidžia labai greitai atlikti daugelį kūrimo ir konfigūravimo veiksmų, naudojant interneto naršyklę.

75. Siūlomas sprendimas turi leisti vystyti/konstruoti tuos pačius aplikacijų komponentus su bet kokio tipo įrankiai, aprašytais aukščiau.
76. Vystymo ir konstravimo įrankiai turi būti pilnai integruoti į sprendimo architektūrą:

    - Saugumo mechanizmai turi būti taikomi tokiu būdu, kad tik atitinkamas autorizacijas turintys naudotojai galėtų atlikti su konstravimu susijusius veiksmus.
    - Artefaktų versijų kontrolės ir diegimo funkcionalumas turi būti integruotas į sistemos vykdymo aplinką.

77. Darbastalio priemonės turi veikti bent trijose skirtingo tipo operacinėse sistemose – Microsoft Windows, Linux, Mac OS X arba lygiavertėse.
78. Internetinės priemonės turi veikti bent trijose skirtingose interneto naršyklėse – Internet Explorer, Firefox, Chrome, Safari arba lygiavertėse.
79. Vystymo/konstravimo įrankiai turi palaikyti daugiamodulinių aplikacijų (DMA) kūrimą, kai skirtingi aplikacijų sluoksniai ir moduliai yra kuriami su skirtingomis technologijomis ir gali būti diegiami skirtingose platformose, tačiau visumoje sudaryti vieningą integruotą aplikaciją.
80. DMA aplikacijų struktūra, įskaitant modulius, savybes, parametrus jei jų tarpusavio priklausomybes turi būti apibrėžta naudojant atviro tipo standartą – YAML arba lygiavertį.
81. DMA turi palaikyti mažiausiai trijų tipų modulius:

    - Duomenų modelio;
    - Veiklos logikos ir taisyklių;
    - Naudotojų sąsajos.

82. Turi būti standartinis procesų modeliavimo įrankis, kurio pagalba tiek techniniai tiek veiklos ekspertai galės modeliuoti ir konstruoti procesus nuo aukščiausio lygio iki žemiausių detalių.
83. Turi būti standartinis veiklos taisyklių kūrimo įrankis, kurio pagalba tiek techniniai tiek veiklos ekspertai (naudojant tiek grafinius tiek tekstinius įrankius) galės:

    - Modeliuoti ir konstruoti taisykles;
    - Aprašinėti ir vykdyti taisyklių testavimo scenarijus;
    - Aprašyti/modeliuoti sprendimų lenteles;
    - Atlikti taisyklių diegimą;

- Aprašyti/modeliuoti taisyklių sekas.

6.2. Reikalavimai duomenų saugai

84. Diegiant programinę įrangą, turi būti laikomasi duomenų saugos reikalavimų, užtikrinančių duomenų konfidencialumą bei apsaugą nuo atsitiktinio ar neteisėto sunaikinimo, naudojimo, atskleidimo, taip pat bet kokio kito neteisėto tvarkymo. Minėtos priemonės turi užtikrinti tokio lygio saugumą, kuris atitiktų saugotinų duomenų pobūdį. Šios priemonės, duomenų saugos tvarkymo reikalavimai ir jų įgyvendinimas nustatyti Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr.716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ reikalavimuose, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. d. įsakymu Nr.1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, Bendruosiuose reikalavimuose organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintuose Valstybinės duomenų apsaugos inspekcijos 2008 m. lapkričio 12 d. direktoriaus įsakymu Nr. 1T-71(1.12, Valstybinės ligonių kasos privalomojo sveikatos draudimo IS SVEIDRA duomenų saugos nuostatuose patvirtintuose, VLK direktoriaus 2007 m. rugsėjo 18 d. įsakymu Nr. 1K-145 (2014 m. gruodžio 22d. įsakymo Nr.1K-371 redakcija), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, apraše patvirtintame Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“, vadovautis VLK direktoriaus 2016 m. liepos 18 d. įsakymu Nr. 222 „Dėl informacijos saugos valdymo sistemos ir informacinių technologijų paslaugų valdymo sistemos nuostatų, taisyklių ir tvarkos aprašų patvirtinimo“ ir kituose teisės, apibrėžiančiuose informacinių sistemų saugumo politiką.
85. Tiekėjo darbuotojai privalės saugoti asmens duomenų paslaptį.
86. Visi Paslaugų teikimo metu panaudoti SSL sertifikatai turi galioti ne trumpesnį, kaip 36 mėnesių laikotarpį, registruoti perkančiosios organizacijos vardu. Sertifikatų kaina turi būti įskaičiuota į pasiūlymo kainą.

6.3. Reikalavimai naudotojo sąsajai

87. SVEIDRA naudotojo sąsaja turi būti prieinama naudojant interneto naršyklę. Naudotojo sąsaja turi būti realizuota lietuvių kalba. IS administratoriams skirti įrankiai turi būti realizuoti lietuvių arba anglų kalba.
88. Sprendimo platforma turi turėti moderniausias naudotojo sąsajos kūrimo galimybes, paremtas HTML5 arba lygiaverte technologija.

89. Naudotojo sąsajos technologijos turi būti pritaikytos skirtingų tipų naudotojų įrenginiams – kompiuteriams, išmaniesiems telefonams bei planšetėms.
90. Naudotojo sąsajos technologijos turi būti paremtos gerai žinomais ir plačiai naudojamais principais – MVC (angl. Model-View-Controller) arba lygiaverčiais principais.
91. Informacijai teikti turi būti naudojami atviri formatai, t.y. oficialiai įregistruoti rinkmenų tarptautiniai standartai (pvz.: HTML, PDF/A, PDF, TIFF, JPEG, PNG, ODF formatai, OOXML formatai, XML ir kt.).
92. SVEIDRA IS naudotojo sąsaja turi būti intuityvi, suprantama ir nesudėtinga naudoti naudotojams, turintiems reikalaujamą kompiuterinio raštingumo lygį (ECDL ar aukštesnį), bei atitikti šiuolaikinius ergonomikos reikalavimus.
93. El. paslaugos turi būti kuriamos vadovaujantis Informacinės visuomenės plėtros komiteto prie Susiekimo ministerijos direktoriaus įsakymu dėl kuriamų viešųjų ir administracinių elektroninių paslaugų tinkamumo naudotojams užtikrinimo priemonių metodinių rekomendacijų patvirtinimo, 2014 m. gegužės 5 d. Nr. T-65
94. Naudotojo sąsajos valdymas turi remtis pelės ir klaviatūros įrenginiais.
95. Naudotojų sąsajos klaidų pranešimai turi būti suformuluoti taip, kad naudotojui būtų aišku, kas atsitiko ir kokius veiksmus jam toliau reikia atlikti, kad galėtų tęsti darbą.
96. Klaidų pranešimuose naudotojams neturi būti pateikiama jokia techninė klaidos informacija (gali būti netaikoma IS administratoriaus rolei). Klaidos pranešime turi būti pateikiamas klaidos identifikatorius, pagal kurį sistemos administratorius gali rasti detalią klaidos techninę informaciją.
97. Duomenų įvedimo formose duomenų laukai turi būti užpildomi automatiškai, jeigu SVEIDRA IS duomenų bazėje ar integruotose duomenų bazėse yra saugomi atitinkami duomenys.
98. Langų bei juose pateikiamų elementų išdėstymas privalo atitikti numatytą jų naudojimo seką.
99. Duomenys, prie kurių naudotojas neturi prieigos teisių, naudotojui privalo būti nepateikiami naudotojo sąsajoje.
100. Informacinėje sistemoje turi būti pažymimi ilgiau trunkantys procesai (funkcijos), kad naudotojui būtų aišku, jog informacinė sistema veikia ir nėra būtinybės iškviesti tų pačių funkcijų keletą kartų.
101. Naudotojas turi būti informuojamas apie sistemos statuso pasikeitimus (kai reikalinga įvestis, būsimų žingsnių peržiūra).
102. Naudotojui pateikiami pranešimai privalo būti lietuvių kalba. Administratoriaus aplinkoje pateikiami pranešimai gali būti lietuvių kalba, anglų kalba.
103. Naudotojui turi būti pateikiami sėkmės pranešimai, nurodantys, kad naudotojo atlikti veiksmai yra sėkmingi (pavyzdžiui, informuojama, kad įrašas išsaugotas/ ištrintas / pakoreguotas, duomenys sėkmingai išsiųsti ir pan.).

6.4. Reikalavimai našumui ir greitaveikai

104. Projektavimo etapo metu Tiekėjas turi identifikuoti ir suderinti su Perkančiąja Organizacija visus našumo ir greitaveikos reikalavimus. Šie reikalavimai turi būti įtraukti į sistemos architektūros prielaidų sąrašą bei į reikalavimų techninei įrangai sąrašą.
105. Šio pirkimo Tiekėjo siūlomas sprendimas ir visa programinė įranga turi būti lanksti ir pritaikoma šiuo metu esantiems bendriems SVEIDRA IS apkrovos rodikliams, taip pat atsižvelgiant į realius naudojimo augimo tempus.
106. SVEIDRA IS užklausų apdorojimo trukmė turi būti racionali užklausos kompleksiškumo atžvilgiu.

107. Siūloma programinė įranga turi turėti galimybę atlikti apkrovų valdymą skirtingose aplinkose, t.y. „įrašant“ apkrovų scenarijų vienoje aplinkoje (pvz. Gamybinėje) ir atkartojant tuos scenarijus kitose aplinkoje (pvz. Testavimo).
108. Apkrovų valdymo funkcionalumas turi veikti su skirtingų versijų DBVS programine įranga, siekiant ištestuoti naujų versijų teikiamus pakeitimus ir jų įtaką greitaveikai.
109. Apkrovų valdymo funkcionalumas turi būti konfigūruojamas tokiu būdu, kuris leistų įjungti/išjungti tam tikras apkrovų scenarijų klases.
110. Sprendimas turi leisti nustatyti našumo parametrus kiekvienai apkrovos klasei. Sistema turi standartiškai sugebėti atpažinti užklausų tipus bei priskirti konkrečiai apkrovos klasei.
111. Turi būti galimybė naudoti standartines bei kurti naujas apkrovos klases, nurodant našumo parametrus.
112. Sprendimas turi leisti konfigūracijos būdu apriboti serverio procesorių resursų panaudojimą (tiek fizinių tiek virtualių) pagal sistemos procesus.

6.5. Reikalavimai plečiamumui

113. Siūlomas sprendimas turi turėti galimybę didinti sistemos našumą kaip vertikalų („scale-up“ - vieno serverio našumo didinimo), taip ir horizontalų („scale-out“- didinant naudojamų serverių skaičių) būdais.
114. Siūlomas sprendimas turi palaikyti šiuos plečiamumo scenarijus visuose trijuose pagrindiniuose sistemos sluoksniuose:

- Duomenų bazėje
- Aplikacijų platformoje
- Integracinėje platformoje

115. Horizontalaus plečiamumo atveju, turi būti galimybė pritaikyti kaip duomenų bazių pasiskirstymo (angl. Partitioning), taip ir duomenų bazių lentelių pasiskirstymo metodiką.
116. Sprendimas turi turėti standartinį įrankį, skirtą duomenų ir lentelių paskirstymui tarp serverių stebėti ir valdyti.
117. Sprendimas turi turėti standartines priemones duomenų ir lentelių paskirstymui tarp serverių keisti. Turi būti galimybė:

- Išsaugoti paskirstymo konfigūraciją
- Atstatyti išsaugotą paskirstymo konfigūraciją
- Atlikti perskirstymą pridedant arba prieš šalinant serverį
- Optimizuoti duomenų ir lentelių paskirstymą automatiniu bei rankiniu būdu

118. Sprendimas turi turėti apkrovos paskirstymo (angl. load balancing) įrankį, kuris sugebėtų automatiškai nuskaityti informaciją apie aplinkos konfigūraciją ir atitinkamai skirstyti užklausas atsižvelgiant į šią informaciją.
119. Sprendimo programinė įranga turi būti sertifikuojama su skirtingų techninės įrangos gamintojų produktais. Šie produktai turi turėti aiškias vertikalaus ir horizontalaus plečiamumo galimybes ir metodikas, siekiant kuo tiksliau įvertinti techninės įrangos poreikius bei kuo efektyviau panaudoti lėšas jos įsigijimui.

6.6. Reikalavimai saugumui

120. Platforma turi palaikyti dviejų tipų tapatybių tiekėjus (angl. Identity providers) – vidinius bei išorinius. Išoriniai tapatybių tiekėjai turi būti lengvai integruojami naudojant standartinį funkcionalumą pagal SAML 2.0 standartą.
121. Platforma turi standartiškai palaikyti trijų tipų naudotojus – programuotojus, administratorius ir galutinius naudotojus.
122. Platforma turi turėti standartines priemones aplikacijoms grupuoti bei izoliuoti nuo kitų aplikacijų techninių resursų, naudotojų ir saugumo prasme. Turi būti galimybė priskirti aplikaciją arba paslaugą prie tam tikros erdvės, tokiu būdu apribojant pasidalinimą techniniais resursais, platformos ar kitokiais servisais bei naudotojais.
123. Autentifikuotos sesijos saugumas turi būti užtikrinamas OAuth 2.0 arba lygiaverčiu standartu.
124. Platforma turi turėti standartines priemones, užtikrinančias apsaugą nuo tokių interneto naršykles išnaudojančių atakų tipų kaip XSS (angl. Cross site scripting), Clickjacking, lokalios saugyklos panaudojimą ir t.t.
125. Platforma turi turėti SSL funkcionalumą duomenų perdavimo apsaugai.
126. Platforma turi turėti konfigūruojamą veiksmų auditavimo funkcionalumą.
127. Veiksmų auditavimo funkcionalumas turi leisti kurti ir valdyti auditavimo politikas, kuriose turi būti galima nustatyti:

- audituojamus įvykius
- audituojamų įvykių baigties būsenas
- audituojamų objektų tipus
- audituojamus naudotojus
- audituojamų įvykių kritiškumą.

128. Veiksmų auditavimo funkcionalumas turi leisti nustatyti tikslinę auditavimo seką kiekvienai atskirai politikai.
129. Kai kurie svarbiausi sisteminiai įvykiai turi būti audituojami pagal nutylėjimą be galimybės išjunti auditavimą.
130. Veiksmų auditavimo funkcionalumas turi leisti rašyti auditavimo sekos informaciją į DB lentelę, failą (CSV arba lygiaverčio formato) arba panaudoti operacinės sistemos galimybes.
131. Sistemos žurnalizavimo funkcionalumas turi turėti atskirus failus kiekvienam aplikacijų platformos moduliui, taip pat turi būti lengvai integruojamas su standartinėmis operacinės sistemos žurnalizavimo priemonėmis.
132. Platforma turi turėti standartinį saugumo sertifikatų valdymo funkcionalumą. Turi būti palaikomas sertifikatų valdymas naudojant failų sistemą bei duomenų bazę.

6.7. Reikalavimai aukštam prieinamumui

133. Sprendimo architektūra turi užtikrinti sistemos aukštą prieinamumą (angl. High availability), kuris gali būti realizuojamas techninės bei programinės įrangos priemonėmis. Modernizuotos SVEIDRA IS aukšto prieinamumas turi atitikti reikalavimus taikomus I kategorijos valstybės informacinėms sistemoms.
134. Aukštas prieinamumas turi būti suprojektuotas ir įgyvendintas duomenų bazių, integracinių sąsajų ir aplikacijų lygiuose.
135. Aukšto prieinamumo sprendimai turi veikti automatiškai (sutrikimo atveju), t.y. žmogaus įsitraukimas turi būti reikalingas tik sistemą atstatant į būseną, kuri buvo prieš sutrikimą. Papildomai turi būti galimybė rankiniu būdu užtikrinti aukštą prieinamumą, jei toks poreikis atsirastų.
136. Perkančioji organizacija įsipareigoja suteikti technologines ir programines priemones, skirtas aukšto prieinamumo užtikrinimui (tarnybinių stočių klasterius, virtualizacijos platformą ir pan.).
137. Programinė įrangą turi turėti standartinį funkcionalumą, kuris stebėtų sisteminių servisų būseną ir atstatinėtų juos, esant sutrikimams.
138. Programinė įranga turi turėti standartinę galimybę realizuoti N+m aukšto prieinamumo klasterį, kuriame m pasyvių dalyvių galėtų perimti visas darbines apkrovas sutrikus vienam (arba daugiau) iš N aktyvių klasterio dalyvių.
139. Sprendimas turi turėti sistemų replikavimo funkcionalumą, kuris leistų greitai atkurti pilną našumą antrinėje sistemoje, įvykus kritiniam pagrindinės sistemos sutrikimui.

6.8. Reikalavimai atsarginių kopijų darymui ir atstatymui

140. Visi duomenų pakeitimai turi būti realiu laiku įrašomi diskų masyve ir šis šaltinis turi būti naudojamas kaip greito pakrovimo rezervinė kopija, sutrikus aplinkos darbui. Šis funkcionalumas turi būti realizuotas tokiu būdu, kad pakrovimas į atmintį po sutrikimo atstatymo būtų kuo greitesnis.
141. Rezervinis duomenų kopijavimas turi būti įmanomas naudojant kaip standartines integruotas siūlomos DBVS priemones taip ir trečiųjų šalių įrankius. Tokiu būdu yra siekiama centralizuotai valdyti visus Perkančiosios organizacijos rezervinio kopijavimo ir atstatymo poreikius.
142. Siūlomai DBVS programinei įrangai ir sprendimui turi egzistuoti DBVS programinės įrangos gamintojo sertifikuoti sprendimai nuotoliniam duomenų replikavimui, siekiant sumažinti bet kokią duomenų praradimo riziką kritinio sutrikimo atveju.
143. Sprendimas turi turėti standartinį funkcionalumą, kuris leistų užtikrinti kad turimos rezervinės kopijos (tiek duomenų, tiek veiksmų žurnalo duomenų, tiek konfigūracijos) yra pakankamos sėkmingam atstatymui atlikti.
144. Sprendimas turi turėti funkcionalumą, kuris sugebėtų nustatyti, kokios atsarginės kopijos jau yra nebereikalingos.
145. Turi būti galimybė apriboti atsarginio kopijavimo ir atstatymo valdymo veiksmus tik tam tikriems naudotojams pasitelkiant sistemos rolių mechanizmą.
146. Sprendimas turi automatiškai nustatyti ir parodyti, kiek vietos diske reikia tolimesniems atsarginio kopijavimo veiksmams atlikti.
147. Sprendimas turi leisti atstatyti sistemos duomenų bazę:

- Iki paskutinės žinomos būsenos;
- Iki tam tikro laiko momento;
- Naudojant tam tikrą pilną atsarginę duomenų kopiją.

6.9. Reikalavimai sprendimo gyvavimo ciklo valdymui

148. Sprendimas turi turėti standartinį pilnai integruotą sistemos gyvavimo ciklo valdymo funkcionalumą, kuris turi užtikrinti vieningą metodologiją bei suteikti reikiamus įrankius visiems sprendimo diegimo etapams – nuo projektavimo iki garantinio aptarnavimo ir palaikymo.
149. Sprendimas turi turėti gyvavimo ciklo valdymo įrankius, veikiančius grafinės naudotojo sąsajos būdu bei komandinės eilutės principu.
150. Sprendimas turi leisti gyvavimo ciklo valdymo funkcionalumo vienetus priskirti naudotojams naudojant standartines roles.
151. Sprendimas turi turėti standartinį komponentų diegimo ir atnaujinimo funkcionalumą, kuris turi maksimaliai automatizuoti su diegimu ir atnaujinimu susijusias užduotis:

    - Komponentų diegimą ir aktyvavimą – sistema turi identifikuoti ar diegiamas komponentas jau yra sistemoje
    - Versijų tikrinimą – sistema turi identifikuoti diegiamo komponento versiją ir palyginti su esamo komponento versija, informuoti apie galimas problemas
    - Klaidų aptikimą – sistema turi fiksuoti ir rodyti visas diegimo metu įvykusias klaidas
    - Pakeitimų atstatymą – sistema turi sugebėti atstatyti sistemą į paskutinę būseną, anuliuojant paskutines diegimo ar atnaujinimo operacijas

152. Sprendimas turi turėti standartinį integruotą pakeitimų perkėlimo tarp sistemų funkcionalumą, siekiant maksimaliai automatizuoti šiuos veiksmus bei sumažinti su tokiais perkėlimais susijusią riziką.
153. Sprendimas turi turėti standartinį integruotą pakeitimų „įrašymo“ funkcionalumą, kuris turi padėti automatiškai atsekti visus pakeitimus aplinkoje bei įtraukti juos į diegimo paketus.
154. Sprendimas turi palaikyti „push“ ir „pull“ pakeitimų perkėlimo mechanizmus.
155. Pakeitimų perkėlimo funkcionalumas turi leisti konfigūruoti sekas, kurios turi nustatyti iš kokios aplinkos bei kokios sistemos bei kokiu būdu ir kokie pakeitimai turi būti perkeliami į esamą sistemą.
156. Sprendimas turi leisti kurti ir valdyti perkėlimo vienetus su galimybė įtraukti bet kokius sistemos konstravimo artefaktus į šiuos vienetus.
157. Turi būti standartinė galimybė perkėlimo vienetus eksportuoti iš vienos aplinkos ir importuoti į kitą.
158. Sprendimas turi turėti standartinį funkcionalumą, kuris leistų automatizuoti perkeliamo ir diegiamo funkcionalumo konfigūravimą sistemoje ir sumažintų rankinio konfigūravimo klaidų riziką.
159. Sprendimas turi turėti standartinį integruotą vertimui skirtą pagalbinį įrankį, kuris leistų eksportuoti iš sistemos visas vertimui skirtas tekstines reikšmes bei importuoti į sistemą išverstas reikšmes.

6.10. Reikalavimai duomenų migravimui

160. Priklausomai nuo pasirinkto modernizavimo sprendimo ir metodikos, Tiekėjas yra atsakingas ir privalo atlikti visų esamų reikalingų duomenų migravimą į modernizuotos sistemos duomenų bazę. Turi būti atliktos visos reikiamos duomenų transformacijos.
161. Turi būti parengtas duomenų migravimo aprašas, kuris minimaliai turi apimti: duomenų migravimo apimčių aprašymą, duomenų transformavimo taisykles, problemų sprendimo mechanizmus, duomenų migravimo technologijas, duomenų integralumo užtikrinimo taisykles, duomenų integralumo testavimo būdą, duomenų migravimo statistiką, detalų duomenų migravimo veiklų grafiką ir pan.
162. Visi detalūs reikalavimai duomenų migravimui turi būti nustatyti detalios analizės etapo metu.

6.11. Reikalavimai programinės įrangos licencijoms

163. Tiekėjų siūloma programinės įrangos licencijos turi būti nuolatinės ir įsigyjamos, o ne nuomos ar panašiu teisiniu pagrindu ar kitaip laiku apribotos: jų galiojimas turi būti nuolatinis ir be pabaigos.
164. Tiekėjų siūloma programinė įranga turi būti instaliuojama Perkančiosios organizacijos valdomoje techninėje įrangoje (angl. on-premise), ir negali būti instaliuota nutolusiuose ne Perkančiosios organizacijos valdomoje techninėje įrangoje, taip vadinamuose debesų sprendimuose (angl. cloud).
165. Siūlomos programinės įrangos licencijos neturi riboti sistemos naudotojų skaičiaus.
166. Tiekėjas turi pasiūlyti licencijų įsigijimo grafiką. Licencijos bus įsigyjamos pagal Tiekėjo pasiūlymą licencijų pateikimo grafiką. Pateikiamos licencijos turi būti pateikiamos kartu su programinės įrangos licencijų gamintojo licencijų palaikymu iki modernizuotos SVEIDRA IS visų modulių pilno įdiegimo ir perdavimo į eksploataciją.
167. Visos Tiekėjų spendimui panaudotos programinės įrangos licencijos privalo turėti gamintojo palaikymą (įskaitant VLK jau turimas licencijas, kurias tiekėjas naudos projekte) iki modernizuotos SVEIDRA IS visų modulių pilno įdiegimo ir perdavimo į eksploataciją.
168. Tiekėjai savo pasiūlyme privalo aiškiai ir nedviprasmiškai nurodyti kokias programinės įrangos licencijas panaudos: tiek Perkančiosios organizacijos jau turimas, tiek ir naujai pateikiamas, taip pat Tiekėjas privalo aiškiai aprašyti programinės įrangos licencijavimo tvarką, gamintojo programinės įrangos licencijų palaikymo tvarką, apmokėjimo už licencijas ir programinės įrangos gamintojo palaikymo tvarką.
169. Siūlomos naudoti programinės įrangos licencijų kaina bei programinės įrangos licencijų gamintojo palaikymo kaina turi būti įskaičiuotą į bendrą pasiūlymo kainą.

6.12. Reikalavimai dokumentacijai

170. Visa dokumentacija turi būti parengta laikantis bendrinės lietuvių kalbos taisyklių.
171. Tiekėjas prieš pradėdamas rengti dokumentus, turi suderinti jų turinį ir apimtis su Perkančiąja organizacija. Detalūs dokumentų derinimo principai turės būti pateikti ir suderinti Tiekėjo parengtame projekto vykdymo reglamente.

172. Turi būti parengtas projekto vykdymo reglamentas, projekto vykdymo planas-grafikas, kokybės valdymo planas, rizikos valdymo planas, konfigūracijos valdymo planas ir kiti planavimo dokumentai. Pastarieji dokumentai gali būti rengiami kaip projekto reglamento turinys ar priedai.
173. Turi būti atlikta esama valstybės informacinės sistemos nuostatų ir saugos nuostatų peržiūra ir esant reikalui parenti sistemos nuostatų ir saugos nuostatų projektai.
174. Turi būti parengtas sistemos Specifikacijos projektas, kuriame apibrėžiami siekiami kompiuterizuoti institucijos veiklos procesai ir jų pokyčiai, aprašomi veiklos reikalavimai valstybės informacinei sistemai.
175. Turi būti parengti Duomenų mainų informacinės sistemos veiklos tęstinumo valdymo plano, duomenų mainų informacinės sistemos naudotojo administravimo taisyklių ir duomenų mainų informacinės sistemos saugaus informacijos tvarkymo taisyklių projektus.
176. Turi būti parengti detalios analizės dokumentai. Detalios analizės dokumente išanalizuojami ir detalizuojami funkciniai ir nefunkciniai techninės specifikacijos reikalavimai bei kiti Perkančiosios organizacijos išsakyti poreikiai, parengiami panaudojimo atvejai (angl. use case), kurie pateikiami panaudos atvejų diagramomis pagal UML (angl. Unified Modeling Language) notaciją ir detalizuojami aprašant kiekvieno panaudos atvejo vykdymo žingsnius (pagrindinę eiga, alternatyvią eigą, išimtinę eigą) ir kitus apribojimus. Sudėtingesni panaudos atvejai ar jų grupės turi būti detalizuojami pateikiant veiklos bei sistemos procesus, naudojant procesų modeliavimo diagramas (UML activity diagram, BPMN (Business Process Model and Notation) ar lygiavertes diagramas). Pateikiami pastarųjų diagramų struktūrizuoti aprašai. Aprašomi sistemos naudotojai ir jų teisės. Turi būti atliktas visų šios specifikacijos funkcinių ir nefunkcinių reikalavimų susiejimas su detalios analizės dokumento turiniu (skyriais, panaudos atvejais, diagramomis ir pan.). Siejimas turi būti atliekamas tokia forma, kad būtų aišku kokiu būdu yra projektuojamas ir realizuojamas kiekvienas šios specifikacijos reikalavimas.
177. Turi būti parengti projektavimo dokumentai. Projektavimo dokumente pateikiama: sistemos architektūros aprašymas fizinių komponentų ir programinių komponentų požiūriu, naudojamos technologijos (jų pavadinimai, versijos), informacinis vaizdas (duomenų bazės struktūros, duomenų bazių sąsajų schemos ir kt.), funkcinis vaizdas (sistemos funkciniai vienetai, jų funkcijos, tarpusavio sąsajos, naudotojo sąsajos prototipai ir kt.), integracinis vaizdas (sąsajos tarp vidinių ir išorinių sistemų, kuriamos sistemos atžvilgiu), operacinis vaizdas (sisteminiai procesai, algoritmai, periodiniai sisteminiai darbai ir pan.), dislokavimo vaizdas (programinių komponentų pasiskirstymas techninėje įrangoje) ir kt.
178. Turi būti parengtos detalios integracinių sąsajų specifikacijos. Jos turi būti suderintos su integruojamų sistemų valdytojais.
179. Turi būti parengta vidinio testavimo ataskaita.
180. Turi būti parengtas priėmimo testavimo planas ir priėmimo testavimo scenarijai. Priėmimo testavimo plane aprašoma testavimo vykdymo metodika, klaidų registravimo tvarka, pateikiami klaidų kritiškumo apibrėžimai, klaidų šalinimo tvarka, aprašoma testavimo aplinka, pateikiamos dalyvių atsakomybės, priėmimo testavimo vykdymo planas-grafikas, priėmimo testavimo užbaigimo kriterijai ir pan. Priėmimo testavimo scenarijuose aprašoma: scenarijaus pavadinimas, sąlygos prieš, sąlygos po, scenarijų vykdančios naudotojų rolės, scenarijaus vykdymo žingsniai ir laukiami rezultatai.
181. Turi būti parengta priėmimo testavimo ataskaita. Ataskaitoje turi būti įvertinti priėmimo testavimo metu nustatyti defektai, pateiktas jų išsprendimo būdas ir statusas, vertinimas sėkmingo priėmimo testavimo kriterijams, pateiktos rekomendacijos dėl tolesnės eksploatacijos.
182. Turi būti parengtas bandomosios eksploatacijos planas. Bandomosios eksploatacijos plane minimaliai turi būti aprašyta: bandomosios eksploatacijos dalyvių komunikavimo schema, dalyvių

atsakomybės, klaidų (pastabų) registravimo tvarka, klaidų šalinimo tvarka, bandomosios eksploatacijos priėmimo kriterijai.

183. Turi būti parengta bandomosios eksploatacijos ataskaita. Bandomosios eksploatacijos ataskaitoje turi būti įvertinti bandomosios eksploatacijos metu nustatyti defektai, pateiktas jų išsprendimo būdas ir statusas, vertinimas sėkmingos bandomosios eksploatacijos kriterijams, pateiktos rekomendacijos dėl tolesnės eksploatacijos.
184. Turi būti parengtas duomenų migravimo dokumentas.
185. Turi būti parengti sistemos naudojimo dokumentai (naudotojų vadovai).
186. Turi būti parengti sistemos administravimo dokumentai (įskaitant ir diegimo instrukciją).
187. Turi būti parengtas garantijos paslaugų suteikimo procedūros dokumentas (įskaitant sistemos pakeitimų valdymo procedūrą).
188. Turi būti parengtas mokymų planas ir mokymų medžiaga.
189. Turi būti parengtos tarpinės paslaugų vykdymo ataskaitos. Tarpinė paslaugų vykdymo ataskaita apima projekto eigos ir rezultatų vertinimą, faktinių rezultatų palyginimą su planu, tolesnių darbų vykdymo planą.
190. Turi būti parengta galutinės diegimo paslaugų vykdymo ataskaita. Galutinė diegimo darbų įvykdymo ataskaita apima projekto eigos ir rezultatų vertinimą, faktinį rezultatų palyginimą su planu ir neatitikimų įvertinimą.
191. Visi Tiekėjo pateikiami dokumentų turi būti pateikiami populiarių standartų failais: xlsx, docx, pptx, pdf.
192. Patvirtinta projekto dokumentacija turi būti pateikiama Perkančiajai organizacijai elektroniniu .pdf formatu bei 2 kopijos popieriniu formatu.

7. Reikalavimai SVEIDRA IS modernizavimo etapų vykdymui

7.1. Reikalavimai projekto valdymui

193. Projekto vykdymo metu VLK paskirs SVEIDRA modernizavimo paslaugų valdymo projekto vadovą ir sudarys jam pavaldžią projekto įgyvendinimo darbo grupę, kurie bus atsakingi už projekto valdymą ir su projekto vykdymu susijusių VLK veiksmų koordinavimą, kontrolę bei atlikimą.
194. Projekto valdymas privalo būti vykdomas vadovaujantis Vykdytojo pateiktu ir su Užsakovu suderintu Projekto valdymo planu, kuris turi būti parengtas atsižvelgiant į Ligonių kasų projektų valdymo tvarkos aprašo, patvirtinto VLK direktoriaus 2016-09-01 įsakymu Nr.1K-254, reikalavimus.

7.2. Reikalavimai testavimui

195. Turi būti atliktas modernizuotos SVEIDRA vidinis testavimas. Vidinius atskirų komponentų testavimus Tiekėjas turi atlikti nedalyvaujant Perkančiosios organizacijos atstovams, tačiau turi pateikti tokio testavimo įrodymus – vidinio testavimo ataskaitą.
196. Turi būti atliktas modernizuotos SVEIDRA priėmimo testavimas. Šis testavimas turi būti atliekamas dalyvaujant Tiekėjui, Perkančiajai organizacijai ir kitoms suinteresuotoms šalims.
197. Priėmimo testavimo tikslai:

- Įsitikinti, kad yra įgyvendinti visi funkciniai ir nefunkciniai reikalavimai.
- Įsitikinti, kad reikalavimai yra įgyvendinti tinkama apimtimi.
- Identifikuoti, užregistruoti ir ištaisyti funkcionalumo klaidas.

198. Atliktas testavimas turi užtikrinti, kad sistema yra tinkama bandomajai eksploatacijai.
199. Priėmimo testavimo metu turi būti vykdomas identifikuotų klaidų (problemų) registravimas.
200. Tiekėjas turės parengti visus testavimui reikalingus testavimo duomenis.
201. Integracinės sąsajos turi būti realizuojamos su integruotinų sistemų testinėmis aplinkomis, jeigu tokios yra. Bandomosios eksploatacijos etape integracinės sąsajos turi būti realizuotos su integruotinų sistemų darbinėmis aplinkomis. Tokios sąsajos privalo būti išbandytos bandomosios eksploatacijos metu.

7.3. Reikalavimai mokymams

202. SVEIDRA naudotojų mokymai turi būti vykdomi atskirais mokymo kursų ciklais pagal mokymo temas. Mokymai turi būti vykdomi Užsakovo patalpose.
203. Tiekėjas turi apmokyti ne mažiau kaip 200 SVEIDRA naudotojų, mokytojų, kurie vėliau apmokys kitus sistemos naudotojus bei 5 sistemos administratorius.
204. Tiekėjas kartu su Perkančiąja organizacija turės parengti bei suderinti mokymų dalyvių sąrašus bei suformuoti mokymų grupes.
205. Mokymų grupės dydis negalės būti didesnis nei 12 asmenų.
206. Tiekėjas privalės prieš programinės įrangos diegimo darbų pradžią parengti, suderinti su VLK mokymo programą bei atlikti mokymus.
207. Reikalavimai programinės įrangos įdiegimo mokymams:

- Tiekėjas paruošia mokymo kursų ciklo metodinės medžiagos paketą, kurį sudaro:
    - Mokymo kursų mokymo programa;
    - Mokymo kursų temos konspektas, kuris pateikiamas kursų dalyviams;
    - Mokymo kursų praktinių darbų užduotys;
    - Mokymo aplinka;
    - Mokymo kursų ciklo tvarkaraštis.
- Mokymai turi būti vykdomi tik VLK patvirtinus mokymo metodinę medžiagą ir suderinus laiką.
- Paslaugos Tiekėjas mokymus turės vykdyti VLK testavimo aplinkoje.

208. Vieno SVEIDRA modulio mokymo trukmė privalo būti ne mažesnė kaip 8 akademinės valandos.
209. Tiekėjas taip pat turės parengti interaktyvią mokymų medžiagą, kuri būtų skirta visiems kitiems sistemos naudotojams ir leistų patiems apsimokinti naudotis modernizuota sistema.
210. Mokymai turi būti vedami lietuvių kalba.

7.4. Reikalavimai bandomajai eksploatacijai

211. Turi būti atlikta modernizuotos SVEIDRA bandomoji eksploatacija.
212. Bandomosios eksploatacijos tikslai:

- Užtikrinti modernizuotos sistemos kokybę.
- Išbandyti gamybinę sistemos konfigūraciją bei stabilizuoti ją, atsižvelgiant į bandomosios eksploatacijos rezultatus.
- Identifikuoti ir pašalinti bandomosios eksploatacijos metu nustatytus defektus.

213. Bandomosios eksploatacijos veiklas Tiekėjas turės vykdyti pagal apibrėžtą bandomosios eksploatacijos planą.
214. Tiekėjas, kartu su Perkančiąją organizacija, iki bandomosios eksploatacijos pradžios privalo paruošti sistemos infrastruktūrą darbui:

- Atlikti sistemos komponentų diegimą ir konfigūravimą.
- Atlikti būtinų duomenų importavimą.

215. Bandomosios eksploatacijos veiklas Tiekėjas turės vykdyti pagal apibrėžtą bandomosios eksploatacijos planą.
216. Tiekėjas privalo užtikrinti modernizuotos SVEIDRA veikimą visos bandomosios eksploatacijos metu.
217. Bandomosios eksploatacijos aplinka turi būti realizuota darbinėje aplinkoje, jeigu nebus sutarta kitaip.
218. Bandomoji eksploatacija yra baigiama, kai tenkinami bandomosios eksploatacijos priėmimo kriterijai, kurie pateikiami bandomosios eksploatacijos plane.

7.5. Reikalavimai garantijos paslaugoms

219. Tiekėjas 12 mėnesių nuo modernizuotos SVEIDROS įvedimo į eksploataciją turi suteikti SVEIDRA informacinės sistemos taikomosios programinės įrangos garantijos paslaugas.
220. Garantijos laikotarpiu Tiekėjas turi užtikrinti šias garantines paslaugas:

- Modernizuotos SVEIDRA IS informacinės sistemos taikomosios programinės įrangos klaidų/trikių ir netikslumų registravimą;
- Modernizuotos SVEIDRA IS programinės įrangos klaidų/trikių ar netikslumų taisymą ir atliktų pakeitimų testavimą, jei klaidos/trikiai ar netikslumai yra atsiradę dėl Tiekėjo kaltės;
- Modernizuotos SVEIDRA IS neatitikimų reikalavimams ir klaidų/trikių šalinimą, jei klaidos/trikiai ar netikslumai yra atsiradę dėl Tiekėjo kaltės;
- Modernizuotos SVEIDRA IS darbingumo atstatymą, pvz., įvykus duomenų bazės ar atskirų jos komponentų darbų sutrikimams, kai tai įvyksta dėl Tiekėjo pateiktų pakeitimų atnaujinimų ar kitų Tiekėjo veiksmų ar neveikimo;
- Išgadintų (sugadintų) duomenų atstatymą, kai gedimo priežastis yra Tiekėjo pateiktos programinės įrangos netinkamas veikimas;
- Modernizuotos SVEIDRA IS techninės dokumentacijos tikslinimą pagal atliktus programinės įrangos pakeitimus;
- Modernizuotos SVEIDRA IS naudotojo vadovo tikslinimą pagal atliktus modernizuotos SVEIDRA IS taikomosios programinės įrangos pakeitimus suteikus garantines paslaugas;

221. Klaidos ir/ar trikiai klasifikuojami:

- kritinė problema – kai nustatytas modifikavimo poreikis arba trikis ir/ar problema, dėl kurios vartotojas negali vykdyti numatytų būtinų funkcijų ir nežinomas joks kitas alternatyvus šios funkcijos vykdymas;
- didelė problema – kai nustatytas modifikavimo poreikis arba trikis ir/ar problema, kuri kliudo vykdyti būtinas funkcijas, tačiau yra žinomas alternatyvus funkcijos vykdymas;
- kita problema – kai nustatytas modifikavimo poreikis arba trikis ir/ar problema, kuri sukelia sunkumus naudojantis programine įranga, bet neįtakoja programinės įrangos funkcijų veikimo ir nedaro jokio kito poveikio programinei įrangai.

222. Tiekėjas privalo analizuoti ir pašalinti problemą arba trikį ir/ar klaidą pagal tokius reikalavimus:

- Reakcijos laikas ir laikas, per kurį tiekėjas turi pašalinti PĮ veikimo problemas:
- 1 (avarija) prioritetas (kai neveikia visa sistema, visi vartotojai negali prisijungti bei atlikti jokių sistemos funkcijų, neleidžiantis prisijungti/naudotis visa sistema visiems; dingsta (ištrinami) visi duomenys) – sutrikimo šalinimas turi būti pradėtas ne vėliau nei per 1 darbo valandas nuo sutrikimo identifikavimo ir turi būti visiškai baigtas ne vėliau nei per 8 darbo valandas;
- 2 (kritinis incidentas) prioritetas (kai vartotojai negali atlikti pagrindinių sistemos funkcijų, neleidžiantis prisijungti/naudotis sistema visiems ar daliai naudotojų; sistema veikia nestabiliai, t.y. pastoviai "lūžta"; metami klaidos pranešimai, reikalaujantys pakartotinio prisijungimo prie sistemos; neteisingai atliekamos operacijos (skaičiavimai); neteisingai išsaugomi duomenys; dingsta (ištrinami) dalis duomenų; nepriimami/neperduodami duomenys kitoms informacinėms sistemoms) – sutrikimo šalinimas turi būti pradėtas ne vėliau kaip per 1 darbo valandas nuo sutrikimo identifikavimo ir turi būti visiškai baigtas ne vėliau nei per 8 darbo valandų (įskaitant laiką, per kuri turi būti pradėtas sutrikimo šalinimas) nuo sutrikimo identifikavimo;
- 3 prioritetas (vidutinės svarbos) (kai pagrindines sistemos funkcijas atlikti galima, tačiau tai yra neįprastai sunku ar nepatogu; (jei kritiniam incidentui yra pasiūlomas apėjimas, funkcijų atlikimas rankomis) taip pat jei visomis sistemos funkcijomis negali naudotis dauguma vartotojų (>50%),) – sutrikimo šalinimas turi būti pradėtas ne vėliau kaip per 1 darbo valandas nuo sutrikimo identifikavimo ir turi būti visiškai baigtas ne vėliau nei per 16 darbo valandų (įskaitant laiką, per kuri turi būti pradėtas sutrikimo šalinimas) nuo sutrikimo identifikavimo;
- 4 (mažos svarbos) prioritetas (kai nepagrindinėmis sistemos funkcijomis negali naudotis mažiau nei pusė vartotojų)– sutrikimo šalinimas turi būti pradėtas ne vėliau kaip per 1 darbo valandas nuo sutrikimo identifikavimo ir turi būti visiškai baigtas ne vėliau nei per 24 darbo valandų (įskaitant laiką, per kuri turi būti pradėtas sutrikimo šalinimas) nuo sutrikimo identifikavimo;.
- 5 (nereikšmingas) prioritetas (kai nepagrindinėmis sistemos funkcijomis negali naudotis keli vartotojai, retai pasikartojančios klaidos) – sutrikimo šalinimas turi būti pradėtas ne vėliau kaip per 1 darbo valandas nuo sutrikimo identifikavimo ir turi būti visiškai baigtas ne vėliau nei per 40 darbo valandų (įskaitant laiką, per kuri turi būti pradėtas sutrikimo šalinimas) nuo sutrikimo identifikavimo

223. Visos modernizuotos SVEIDRA IS garantinės paslaugos turės būti priderintos prie VLK IT pagalbos tarnybos (http:// itpagalba.vlk.lt).

224. Visos sukurtos sistemos programinės įrangos komponentų pasiekiamumas turi būti ne mažesnis nei 99 % procentų laiko per metus.