

**LIETUVOS RESPUBLIKOS UŽSIENIO REIKALŲ MINISTERIJOS
KASDIENĖS UŽSIENIO REIKALŲ MINISTERIJOS INFORMACIJOS
POSISTEMIO (KURMIS) PALAIKymo IR VYSTYMO PASLAUGŲ
TECHNINĖ SPECIFIKACIJA**

1. BENDROSIOS NUOSTATOS

Lietuvos Respublikos užsienio reikalų ministerija (toliau – URM arba Perkančioji organizacija) siekia įsigyti Kasdienės Užsienio reikalų ministerijos informacijos posistemio (toliau – KURMIS) priežiūros ir vystymo paslaugas.

Naudojamos santrumpos:

Santrumpa	Paaiškinimas
KURMIS	Kasdienės Užsienio reikalų ministerijos informacijos posisemis
TVS	Turinio valdymo sistema
URM, Perkančioji organizacija	Lietuvos Respublikos užsienio reikalų ministerija
URMIS	Lietuvos Respublikos užsienio reikalų ministerijos informacinė sistema

2. ESAMOS SITUACIJOS APRAŠYMAS

2.1. Esama aplinka

2.1.1. Informacija KURMIS teikiama lietuvių kalba.

2.1.2. KURMIS paskirtis:

2.1.2.1. URM ir Lietuvos Respublikos diplomatinių atstovybių ir konsulinių įstaigų, atstovybių tarptautinėse organizacijose ir specialiųjų misijų (toliau – atstovybės) darbuotojų tarpusavio komunikacijos plėtojimas;

2.1.2.2. Sąlygų operatyviai gauti aktualią URM ir atstovybių informaciją, kurios reikia darbo funkcijoms atlikti, sudarymas;

2.1.2.3. Neformalių URM ir atstovybių darbuotojų ryšių stiprinimas.

2.1.3. KURMIS funkcijos:

2.1.3.1. Komandinis dokumentų valdymas ir jų skelbimas autorizuotiems naudotojams;

2.1.3.2. Informacijos skelbimas ministerijos viduje;

2.1.3.3. Bendro kalendoriaus naudojimas;

2.1.3.4. Darbuotojų tarpusavio komunikacija;

2.1.3.5. Bendras ministerijos, padalinių ir darbo grupių socialinis tinklas;

2.1.3.6. Informacija apie naudotojus;

2.1.3.7. Žiniasklaidos naujienų srautas.

2.2. KURMIS programinė ir techninė charakteristikos

Naudojama programinė įranga	Techninės įrangos parametrai	Integracinės sąsajos
- Centos 8.1 - Programavimo kalba – PHP 7.4 - Duomenų bazės platforma – MariaDB 10.3 - Turinio valdymo sistema SystemSight	4Cpu, 12GB RAM	KURMIS integracinė sąsaja su URM Personalo valdymo sistema duomenų mainais XML formatu.

3. BENDRIEJI REIKALAVIMAI PASLAUGOMS IR JŲ VALDYMOUI

3.1.	Bendrieji reikalavimai
3.1.1.	Paslaugų teikėjas turi užtikrinti, kad visa komunikacija Sutarties vykdymo metu vyktų lietuvių kalba. Jei pasitelkiami užsienio šalių ekspertai, Paslaugų teikėjas turi pasirūpinti vertimo į lietuvių kalbą paslaugomis.
3.1.2.	Paslaugos turi būti teikiamos 12 mėnesių nuo KURMIS vystymo ir priežiūros paslaugų sutarties (toliau – Sutartis) įsigaliojimo dienos su galimybe pratęsti du kartus po 12 mėnesių.
3.1.3.	Papildomos KURMIS vystymo paslaugos, nurodytos šios Techninės specifikacijos 4.1. papunktyje, turi būti teikiamos pagal Perkančiosios organizacijos poreikį visą Sutarties galiojimo laikotarpį.
3.1.4.	KURMIS priežiūros paslaugos, nurodytos šios Techninės specifikacijos 4.2. papunktyje, turi būti teikiamos pagal Perkančiosios organizacijos poreikį visą Sutarties galiojimo laikotarpį.
3.1.5.	Paslaugų teikėjas turi paskirti iš savo pusės Projekto vadovą, kuris būtų atsakingas už susitikimų organizavimą ir komunikaciją tarp Paslaugų teikėjo ir Perkančiosios organizacijos. Projekto vadovui nesant darbe ar jam laikinai negalint atlikti savo darbo funkcijų, jį turi pavaduoti kitas Paslaugų teikėjo paskirtas darbuotojas. Apie laikinai paskirtą Projekto vadovą pavaduojantį darbuotoją Paslaugų teikėjas nedelsiant turi informuoti Perkančiąją organizaciją. Komunikavimas, darbo funkcijų vykdymas ir kiti darbai negali nutrūkti dėl darbuotojo nebuvimo darbe.
3.1.6.	Visi Projekto metu sukurti ir įgyti rezultatai ir su jais susijusios teisės, Paslaugų teikėjo sukurtos vykdant Sutartį, įskaitant autorių ir kitas intelektinės ar pramoninės nuosavybės teises, yra Perkančiosios organizacijos nuosavybė, kurią ji gali naudoti, publikuoti, disponuoti kaip mano esant tinkama ir be jokių apribojimų.
3.1.7.	Projekto metu Paslaugų teikėjui, su Perkančiąja organizacija suderintu laiku, darbų vykdymui ribotam laikui gali būti suteikta nuotolinė prieiga iš fiksuotų IP adresų prie KURMIS aplinkos.
3.1.8.	Paslaugų teikėjas turi užtikrinti, kad jokios testinės KURMIS versijos nebus prieinamos trečiosioms šalims be Perkančiosios organizacijos sutikimo.

4. NEFUNKCINIAI REIKALAVIMAI

4.1.	Reikalavimai priežiūros ir vystymo paslaugoms
4.1.1.	Perkančioji organizacija numato pagal poreikį įsigyti KURMIS palaikymo ir vystymo paslaugas (toliau – paslaugos). Numatomas paslaugų valandų kiekis yra 1500 val. Perkančioji organizacija neįsipareigoja įsigyti viso valandų kiekio.
4.1.2.	Visą Sutarties galiojimo laikotarpį, jeigu netaikomas garantinis aptarnavimas, Paslaugų teikėjas turi teikti šias priežiūros paslaugas: • Užtikrinti KURMIS veiklos atkūrimą visiško arba dalinio funkcionavimo sutrikimo atvejais, įskaitant sutrikimus, atsiradusius dėl klaidų programinėje įrangoje; • Atstatyti sugadintus programinės įrangos komponentus ir duomenis; • Taisyti aptiktas saugumo klaidas TVS; • Konsultuoti Perkančiosios organizacijos darbuotojus darbo su TVS, informacijos talpinimo į TVS ir jos konfigūravimo klausimais, kurių atsakymai nereikalauja papildomos programinės įrangos duomenų analizės. Perkančiosios organizacijos darbuotojai konsultuojami Perkančiosios organizacijos darbo laiku telefonu ir elektroniniu paštu.
4.1.3.	Sutarties galiojimo laikotarpiu Perkančioji organizacija gali įsigyti, bet neapsiriboti, šiomis KURMIS vystymo paslaugomis: • KURMIS TVS atnaujinimas iki naujausios versijos ne rečiau kaip vieną kartą per metus arba esant poreikiui (pvz. atsiradus kritiniams pažeidžiamumams); • KURMIS PHP atnaujinimas iki naujausios versijos ne rečiau kaip vieną kartą per metus arba esant poreikiui (pvz. atsiradus kritiniams pažeidžiamumams) (įskaitant PHP versijos atnaujinimus serveryje); • Duomenų bazės atnaujinimas iki naujausios versijos ne rečiau kaip vieną kartą per metus arba esant poreikiui (pvz. atsiradus kritiniams pažeidžiamumams) (įskaitant versijos atnaujinimus serveryje); • KURMIS programinio karkaso (angl. <i>framework</i>) atnaujinimas iki naujausios versijos ne rečiau kaip vieną kartą per metus arba esant poreikiui (pvz. atsiradus kritiniams pažeidžiamumams); • Funkcinių naujinių sukūrimas, vystymas, diegimas ir priežiūra arba esamo funkcionalumo papildymas; • KURMIS naujo dizaino kūrimas arba esamo dizaino tobulinimas, KURMIS dizaino elementų kūrimas ir integravimas su TVS.
4.1.4.	Vystymo paslaugos turi būti teikiamos laikantis šioje Techninėje specifikacijoje numatytų reikalavimų.
4.1.5.	KURMIS priežiūros metu visos atsiradusios ir nustatytos klaidos, trikdžiai, sutrikimai ir problemos turi būti klasifikuojami į: • Kritinės klaidos atveju (visa TVS, svetainė ar atskiros jos dalys neveikia, posisemis nepasiekiamas naudotojams) – ne ilgesnis kaip 4 val. darbo dienomis; • Vidutinės svarbos klaidos atveju (neveikia vienas ar keli TVS, svetainės moduliai/blokai, kitos dalys veikia korektiškai) – ne ilgesnis kaip 8 val. darbo dienomis; • Klaidos atveju (posistemo veikimas neatitinka pirkimo sutartyje nustatytų reikalavimų, nedideli dizaino neatitikimai) – ne ilgesnis kaip 2 darbo dienos.

4.1.	Reikalavimai priežiūros ir vystymo paslaugoms
4.1.6.	Pagrindinės priežiūros sąlygos: • Kritinės klaidos atveju – ne ilgesnis kaip 4 val. darbo dienomis; • Vidutinės svarbos klaidos atveju – ne ilgesnis kaip 8 val. darbo dienomis; • Klaidos atveju – ne ilgesnis kaip 24 val. darbo dienomis. Galimybė visą parą registruoti problemas internetu bei stebėti problemų sprendimo būklę naudojant Paslaugų teikėjo pateiktą klaidų registravimo įrankį.
4.1.7.	Užsakymo vystymo paslaugoms pateikimas vykdomas per pasirinktą komunikavimo kanalą. Paslaugų teikėjas ne vėliau kaip per 5 darbo dienas pateikia užsakymo įvykdymo terminą, taip pat užsakymo įgyvendinimo valandas ir sumą. Perkančioji įstaiga ne vėliau kaip per 3 darbo dienas patvirtina / atmeta užsakymą. Įvykdymo terminas negali būti ilgesnis nei buvo numatytas, nebent, susiderinus su Perkančiąja organizacija, terminas bus pratęstas. Vienašališkai Paslaugų teikėjas negali pratęsti termino. Priežiūros metu Paslaugų teikėjas privalo registruoti KURMIS eksploatavimo sutrikimus ir neatitiktis problemų / sutrikimų registravimo sistemoje (pvz., specializuotoje interneto svetainėje arba per pagalbos teikimo liniją (angl. <i>Service Desk</i>) pagal su Perkančiąja organizacija suderintas informavimo ir registravimo procedūras.
4.1.8.	Priežiūros ir vystymo paslaugų laiko sąnaudos valandomis apvalinamos 15 minučių tikslumu.

4.2.	Reikalavimai garantiniam aptarnavimui
4.2.1.	KURMIS vystymo ir priežiūros paslaugoms, nurodytoms šios Techninės specifikacijos 4.1. papunktyje, turi būti suteiktas 12 mėn. garantinis aptarnavimas nuo konkrečių vystymo ar priežiūros paslaugų priėmimo-perdavimo akto pasirašymo dienos.
4.2.2.	Garantinio aptarnavimo metu Paslaugų teikėjas privalo: • Užtikrinti KURMIS veiklos atkūrimą visiško arba dalinio funkcionavimo sutrikimo atvejais, įskaitant sutrikimus, atsiradusius dėl klaidų standartinėje (Paslaugų teikėjo įdiegtoje, tačiau sukurtoje kažkieno kito) ir nestandartinėje (Paslaugų teikėjo sukurtoje ar modernizuotoje) programinėje įrangoje (išskyrus atvejus, atsiradusius dėl Perkančiosios organizacijos kaltės); • Atstatyti sugadintus programinės įrangos komponentus ir duomenis (išskyrus atvejus, atsiradusius dėl Perkančiosios organizacijos kaltės); • Nemokamai taisyti sukurtos ar modifikuotos programinės įrangos, duomenų mainų sąsajų bei kitų sukurtų ar modifikuotų sprendimų klaidas, netikslumus ir neatitikimus Techninėje specifikacijoje apibrėžtiems reikalavimams, taip pat parengti, ištestuoti ir paruošti diegimui reikalingus atnaujinimus.
4.2.3.	Garantinio aptarnavimo metu Paslaugų teikėjas privalo registruoti KURMIS eksploatavimo sutrikimus ir neatitiktis problemų / sutrikimų registravimo sistemoje (pvz., specializuotoje interneto svetainėje arba per pagalbos teikimo liniją (angl. <i>Service Desk</i>) pagal su Perkančiąja organizacija suderintas informavimo ir registravimo procedūras.
4.2.4.	Reakcijos (atsakymo) laikas po pranešimo apie gedimą: • Kritinės klaidos atveju (visa TVS, svetainė ar atskiros jos dalys neveikia, posistemis nepasiekiamas naudotojams) – ne ilgesnis kaip 4 val. darbo dienomis;

4.2.	Reikalavimai garantiniam aptarnavimui
	• Vidutinės svarbos klaidos atveju (neveikia vienas ar keli TVS, svetainės moduliai/blokai, kitos dalys veikia korektiškai) – ne ilgesnis kaip 8 val. darbo dienomis; • Klaidos atveju (posistemio veikimas neatitinka pirkimo sutartyje nustatytų reikalavimų, nedideli dizaino neatitikimai) – ne ilgesnis kaip 2 darbo dienos.
4.2.5.	Gedimų pašalinimo laikas: • Kritinės klaidos atveju – ne ilgesnis kaip 4 val. darbo dienomis; • Vidutinės svarbos klaidos atveju – ne ilgesnis kaip 8 val. darbo dienomis; • Klaidos atveju – ne ilgesnis kaip 24 val. darbo dienomis.

4.3.	Reikalavimai diegimui
4.3.1.	KURMIS turi turėti analogišką testavimo aplinką, kuri naudojama testavimui, administratorių ir naudotojų mokymui. Testavimo aplinka turi būti išlaikyta iki pirkimo sutarties galiojimo pabaigos.
4.3.2.	Prieš diegiant naujus funkcionalumus į produkcinę aplinką, jie turi būti įdiegti ir ištestuoti testinėje aplinkoje. Tik Perkančiajai organizacijai patvirtinus, nauji funkcionalumai gali būti diegiami produkcinėje aplinkoje.
4.3.3.	Diegimas turi būti vykdomas tuo metu, kai KURMIS naudojamumas yra mažiausias Perkančiosios organizacijos darbo valandomis. Darbų atlikimo laikas (grafikas) turi būti suderintas su Perkančiąja organizacija.
4.3.4.	Paslaugų teikėjas turi užtikrinti galimybę atstatyti KURMĮ ir visus jo duomenis į būseną iki diegimo, jei diegimas būtų nesėkmingas ir būtų prarasti ir / ar sugadinti KURMIS duomenys ir / ar funkcijos (pvz., esant poreikiui, Paslaugų teikėjas iki diegimo pradžios turėtų paruošti pilną KURMIS (ar jos dalies / modulio / elemento) ir jos duomenų kopiją).
4.3.5.	Diegimo etapo metu į produkcinę aplinką turi būti diegiami tik tie pakeitimai, kurie nedaro įtakos kitiems KURMIS komponentams, yra ištestuoti ir yra pilnai veikiantys.
4.3.6.	Diegimas į testinę bei produkcinę aplinkas vykdomas Perkančiosios organizacijos darbo laiku: pirmadienis–ketvirtadienis 08.00–17.00 val., penktadienis 08.00–15.45 val.

4.4.	Reikalavimai dokumentacijai
4.4.1.	Visa Paslaugų teikėjo rengiama dokumentacija turi būti parengta lietuvių kalba, vadovaujantis bendrinėmis lietuvių kalbos taisyklėmis.
4.4.2.	Dokumentų galutinės versijos turi būti pateiktos redagavimui tinkamu (.doc, .docx, .pdf arba kitu su Perkančiąja organizacija suderintu) elektroniniu formatu.
4.4.3.	Atliekant sistemos vystymo darbus turi būti atnaujinta: • KURMIS specifikacija; • Sąsajų tarp sistemų (angl. <i>interface</i>) ir jų valdymo bei funkcinių sričių aprašymas; • TVS administratorių ir naudotojų vadovai. Perkančioji organizacija savo nuožiu gali paprašyti pateikti papildomus, šiame punkte nenurodytus, dokumentus arba atsisakyti vieno ar kelių dokumentų rengimo.

4.4.	Reikalavimai dokumentacijai
4.4.4.	Visos sutarties metu Paslaugų teikėjo parengta dokumentacija turi būti atnaujinama taip, kad pateikti aprašymai atitiktų realią KURMIS būseną (su visais garantinio aptarnavimo metu įdiegtais pakeitimais).

4.5.	Reikalavimai saugumui
4.5.1.	Duomenų sauga turi būti užtikrinta vadovaujantis asmens duomenų apsaugą reglamentuojančiais dokumentais ir reikalavimais:
4.5.1.1.	Europos parlamento ir tarybos reglamentu (ES) 2016/679 2016 m. balandžio 27 d. dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendruoju duomenų apsaugos reglamentu).
4.5.1.2.	Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu.
4.5.1.3.	Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Vyriausybės 2018 m. rugpjūčio 13 nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.
4.5.1.4.	Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“.
4.5.1.5.	URMIS saugos politikos reikalavimais, nustatytais Lietuvos Respublikos užsienio reikalų ministerijos informacinių sistemų duomenų saugos nuostatuose, patvirtintuose Lietuvos Respublikos užsienio reikalų ministro 2022 m. vasario 23 d. įsakymu Nr. V-54 „Dėl Lietuvos Respublikos užsienio reikalų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“.
4.5.1.6.	Lietuvos Respublikos užsienio reikalų ministro 2022 m. gegužės 5 d. įsakymu Nr. V-163 patvirtintomis Lietuvos Respublikos užsienio reikalų ministerijos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėmis.
4.5.1.7.	OWASP programinės įrangos saugos užtikrinimo standartu (angl. OWASP Application Security Verification Standard 4.0.3.)
4.5.1.8.	OWASP Saugaus programavimo gairėmis (angl. OWASP SCP Quick Reference Guide v).
4.5.2.	Sistema turi būti atspari slaptažodžių parinkimo (angl. brute force) atakoms. Jei naudotojas neteisingą slaptažodį įveda daugiau kartų nei leista, toks naudotojas turi būti blokuojamas ir apie tokį įvykį turi būti informuoti administratoriai.
4.5.3.	Sistema turi užtikrinti veikimą naudojantis HTTPS saugiu protokolu.
4.5.4.	Kai naudotojai prie sistemos bando jungtis nesaugiu (nešifruotu) kanalu, sistema privalo tai fiksuoti ir informuoti administratorius arba įrašyti tai į įvykių žurnalą.
4.5.5.	Jungiantis HTTP protokolu, naudotojas turi būti nukreipiamas į sistemą HTTPS protokolu.
4.5.6.	Jungiantis prie sistemos turinio valdymo administravimo aplinkos turi būti naudojamas tik saugus HTTPS ryšys.

4.5.	Reikalavimai saugumui
4.5.7.	Turi būti kaupiama informacija apie visus administratorių ir redaktorių prisijungimus bei atliekamus redagavimo veiksmus. Laikotarpio, už kurį kaupiama informacija, trukmė turi būti konfigūruojama sistemos nustatymuose.
4.5.8.	Sistema duomenų perdavimui tarp sistemos naudotojo darbo stoties ir sistemos tarnybinės stoties privalo naudoti šifruotą ryšio kanalą. Ryšio kanalo šifravimui turi būti naudojama SSL (angl. Secure Socket Layer) technologija.
4.5.9.	Sistema privalo neleisti vykdyti XSS (angl. Cross Site Scripting) atakas, neleidžiant nusiųsti į serverį žalingo HTML ar Javascript kodo, arba teisingai tokį siuntimą apdoroti (angl. encode), tam, kad nebūtų paveikti kiti sistemos naudotojai.
4.5.10.	Serverio administravimo lygmenyje turi būti naudojama SSH (angl. Secure shell).
4.5.11.	Sistema turi būti apsaugota nuo:
4.5.11.1.	Neautentifikuotos prieigos.
4.5.11.2.	Nesankcionuoto naudotojo sesijos perėmimo.
4.5.11.3.	Nesankcionuoto duomenų perėmimo ar jų įterpimo.
4.5.11.4.	Nuo SQL injekcijų į duomenų bazę.
4.5.12.	Pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. The Open Web Application Security Project (OWASP)) interneto svetainėje www.owasp.org .
4.5.13.	Duomenų bazėje turi būti naudojamos parametrizuotos SQL užklausos.
4.5.14.	Turi būti realizuotas sprendimas, leidžiantis administruoti TVS tik jungiantis iš nurodytų IP adresų nurodant konkretų adresą ar rėžį.
4.5.15.	Realizuotas dvigubos autentifikacijos sprendimas administratoriams.
4.5.16.	Paslaugų teikėjas kurdamas testinę (programavimo) aplinką Perkančiosios organizacijos sistemai savo aplinkoje, užtikrina, kad šią aplinką pasieks tik darbuotojai, dalyvaujantys projekte, ir Perkančiosios organizacijos darbuotojai, iš aprašytų ir su Perkančiąja organizacija suderintų IP adresų.
4.5.17.	Prisijungimai prie TVS sistemos turi būti fiksuojami ir saugomi (įskaitant ir nesėkmingus bandymus prisijungti).
4.5.18.	Naudojant atviro kodo TVS, Paslaugų teikėjas turi užtikrinti saugų jos naudojimą (reguliarus atnaujinimų diegimas, patikimų įskiepių naudojimas, kita).
4.5.19.	Turi būti uždrausta prieiga prie objektų, kurie atskleidžia perteklinę informaciją.
4.5.20.	Turi būti realizuotas informacijos kaupimas apie sistemos klaidas su galimybe jas peržiūrėti.
4.5.21.	Duomenų bazė turi būti naujinama, plečiama, taikant gerąsias duomenų bazių praktikas:
4.5.21.1.	Turi būti realizuotos duomenų vientisumą užtikrinančios priemonės (apribojimų (angl. <i>constraints</i>) naudojimą, normalinių formų pritaikymą).
4.5.21.2.	Turi būti realizuotos konfidencialumą užtikrinančios priemonės (turi būti užtikrintas slaptažodžių saugumas juos koduojant vienpusio kodavimo algoritmu su druska (angl. salt), slaptažodis neturi būti saugomas duomenų bazėje, saugomas tik jo mišinys (angl. hash)). Slaptažodžiai negali būti saugomi atviru tekstu (angl. plain text), ar koduojant visuotinai pripažintais nesaugiais šifravimo algoritmais (pavyzdžiui, MD5).
4.5.21.3.	Turi būti registruojami bandymai nesankcionuotai patekti, įsilaužti į sistemą.
4.5.21.4.	Turi būti konfigūruotas ir pateikta instrukcija apie duomenų bazės rezervinį kopijavimą ir atstatymą duomenų bazės priemonėmis.

4.5.	Reikalavimai saugumui
4.5.22.	Visi bandymai neteisėtai pasinaudoti prieiga prie sistemos ir jos duomenų turi būti atvaizduojami tokių įvykių registravimo žurnale. Taip pat sistemos administratoriui turi būti siunčiamas pranešimas (el. laiškas ir sisteminis pranešimas) iškart identifikavus tokį įvykį.
4.5.23.	Elektroninė informacija atsarginėse kopijose turi būti užšifruota arba turi būti imtasi kitų priemonių, užtikrinančių atsarginėse kopijose esančios informacijos saugumą.
4.5.24.	Turi būti realizuotas funkcionalumas administravimo aplinkoje nustatyti naudotojo slaptažodžio politiką (slaptažodžio ilgį, kompleksiskumą (didžiosios, mažosios raidės, skaičiai, spec. simboliai), slaptažodžio galiojimo terminas ir privalomas keitimas jam pasibaigus, nesikartojančių slaptažodžių kiekis, neaktyvių paskyrų blokavimas po nustatyto laiko, bei dviejų faktorių autentifikavimas).
4.5.25.	Administratorius gali nustatyti reikalavimus slaptažodžiui: ilgis, simbolių tipai ir kita.
4.5.26.	Po svetainės įdiegimo užsakovo iniciatyva atliekamas svetainės ir svetainėje naudojamų komponentų saugos testavimas. Identifikavus svetainėje naudojamo programinio kodo pažeidžiamumus Tiekėjas privalo juos ištaisyti.
4.5.27.	Turi būti laikomasi šių viešai prieinamų svetainių kriptografiniams raktams ir algoritmams taikomų reikalavimų: • naudojamas TLS 1.2 ir aukštesnis kriptografinis protokolas. Draudžiama naudoti TLS1.0, TLS 1.1 ir SSL3 dėl žinomų ir plačiai išnaudojimų pažeidžiamumų; • sertifikato šifravimo/maišos funkcijai naudojamas SHA2 ir aukštesnis algoritmas.
4.5.28.	Perkančioji organizacija turi teisę reikalauti, kad Paslaugų teikėjas pateiktų įrodymus, jog yra laikomasi nustatytų informacijos saugumo reikalavimų, taip pat tikrinti teikėjo paslaugų teikimo procesą, siekiant įsitikinti šių reikalavimų laikymąsi.