

URM IR DIPLOMATINIŲ ATSTOVYBIŲ SVETAINIŲ IR TURINIO VALDYMO SISTEMOS PALAIKYMŲ IR VYSTYMO PASLAUGŲ TECHNINĖ SPECIFIKACIJA

Pirkimo tikslas. Lietuvos Respublikos užsienio reikalų ministerija (toliau – Perkančioji organizacija) siekia įsigyti Lietuvos Respublikos užsienio reikalų ministerijos interneto svetainės (<https://urm.lt>) (toliau – URM svetainė) ir Lietuvos Respublikos diplomatinės atstovybių užsienio valstybėse, Lietuvos Respublikos atstovybių prie tarptautinių organizacijų, konsulinės įstaigų ir specialiųjų misijų (toliau – DA) interneto svetainių ir šablono (toliau – šablonas DA svetainėms) (kartu toliau – URM svetainės) palaikymo ir vystymo paslaugas.

Svetainių paskirtis. URM svetainė ir DA svetainės yra vienas svarbiausių Perkančiosios organizacijos komunikacijos viešojoje erdvėje įrankių. Svetainės skirtos Perkančiosios organizacijos veiklos viešinimui ir visuomenės informavimui. Informacija URM svetainėje pateikiama 5 kalbomis: lietuvių, anglų, rusų, lenkų ir prancūzų, DA svetainėse – lietuvių ir keliomis užsienio kalbomis priklausomai nuo valstybės, kurioje įsikūrusi DA.

Svetainių tikslinės grupės (lankytojai). URM svetainė naudojasi Lietuvos Respublikos gyventojais, užsieniečiais, valstybinės institucijos, nevyriausybinių organizacijų, asocijuotos ir verslo struktūros, žurnalistai ir visi kiti, besidomintys užsienio politika. DA svetainėmis daugiausiai naudojasi užsienyje keliaujantys ar gyvenantys Lietuvos Respublikos piliečiai ir užsieniečiai.

Tikslas. Palaikyti ir vystyti Lietuvos Respublikos užsienio reikalų ministerijos ir Lietuvos diplomatinės atstovybių svetainių šabloną, pagal poreikį vykdyti kitus svetainių vystymo darbus, kurie turi atitikti valstybės institucijų svetainėms keliamus saugumo ir kitus reikalavimus.

URM svetainės priežiūros ir vystomos pagal žemiau nurodytus techninius reikalavimus.

Eil. Nr.	1. BENDRIEJI REIKALAVIMAI
1.1.	Numatomos sudaryti pirkimo sutarties trukmė – 12 mėnesių nuo pirkimo sutarties įsigaliojimo dienos. Paslaugas tiekėjas privalo teikti šiais terminais: • TVS, URM svetainės ir DA svetainių palaikymo ir vystymo paslaugos turi būti teikiamos nuo pirkimo sutarties pasirašymo dienos iki pirkimo sutarties galiojimo pabaigos.
1.2.	Visų modulių galutinis funkcionalumas, reikalingi laukai ir parametrai bei veikimo principai turi būti suderinti su Perkančiąja organizacija.
1.3.	URM svetainė turi atitikti bendruosius reikalavimus, pateiktus valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2021 m. gruodžio 1 d. nutarimu Nr. 1015 „Dėl bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms ir mobiliosioms programoms aprašo patvirtinimo“ ir Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013 m. gegužės 23 d. įsakymu Nr. T-72 „Dėl informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos vyriausybės direktoriaus 2004 m. kovo 31 d. įsakymo Nr. T-40 „Dėl neįgaliesiems pritaikytų interneto tinklalapių kūrimo, testavimo ir įvertinimo metodinių rekomendacijų patvirtinimo“ pakeitimo“ patvirtintų rekomendacijų nuostatas.
1.4.	URM svetainė ir TVS turi turėti analogišką testavimo aplinką, kuri naudojama testavimui ir administratorių ir naudotojų mokymui. Testavimo aplinka turi būti išlaikyta iki pirkimo sutarties galiojimo pabaigos.
1.5.	URM svetainėse ir šablone DA svetainėms negali būti nuorodos į Tiekėjo interneto svetainę bei kitos

	Tiekėjo reklamos.
1.6.	Perkančioji organizacija turi laike neribotą teisę be papildomo atlygio naudoti Perkančiajai organizacijai sukurtą programinę įrangą; teisę daryti sukurtos programinės įrangos kopijas; teisę modifikuoti ir toliau plėtoti sukurtą programinę įrangą; teisę perkelti programinę įrangą į kitą technologinę platformą; suteikti teises naudoti šią programinę įrangą kitoms trečiosioms šalims; teisę naudoti ir keisti Pirkėjui sukurtos programinės įrangos pradinį kodą.
1.7.	Komunikavimas bei instrukcija turi būti vykdomas / pateikta lietuvių kalba.
1.8.	Planuojama įsigyti: • XXX val. TVS, URM svetainės ir šablono DA svetainėms palaikymo bei vystymo ir dizaino paslaugas. Perkančioji organizacija neįsipareigoja nupirkti viso kiekio valandų.
1.9.	URM ir DA svetainės turi veikti 24/7 (24 valandos per parą, 7 dienos per savaitę) režimu. URM ir DA svetainių funkcionalumas turi veikti ne mažiau kaip 95% laiko per metus.
1.10.	Tiekėjas turi užtikrinti URM ir DA svetainių nenutrūkstamą veikimą, priklausantį nuo TVS, programinio kodo, duomenų bazės ir kitų svetainės programinių modulių. URM ir DA svetainių tarnybinių stočių infrastruktūros nenutrūkstamą veikimą užtikrina pati Perkančioji organizacija.
1.11.	Tiekėjas turi būti pasiekiamas Perkančiosios organizacijos darbo valandomis, t. y. nuo 8 val. iki 17 val. pirmadieniais – ketvirtadieniais ir nuo 8 val. iki 15.45 val. penktadieniais.
1.12.	Tiekėjui bus suteikiama ribota nuotolinė prieiga pagal Perkančiosios organizacijos saugos politiką. Tiekėjas galės visą pirkimo sutarties galiojimo laikotarpį suderintu laiku ir iš suderintų IP adresų jungtis nuotoliniu būdu į testinę ir/ar produkcinę aplinką arba paslaugos galės būti suteikiamos, atvykus į Perkančiosios organizacijos patalpas, adresu, J. Tumo-Vaižganto g. 2, Vilnius, Lietuva.

Eil. Nr.	2. REIKALAVIMAI PRIEŽIŪRAI
2.1.	Tiekėjas turi teikti TVS, URM svetainės ir DA svetainių priežiūros paslaugas.
2.2.	Tiekėjas turi paskirti atsakingą asmenį, per kurį bus vykdomas komunikavimas (vystymo paslaugų užsakymas, gedimų registracija, konsultacijos, kita). Paskirtam asmeniui susirgus ar kitaip negalintį atlikti minėtų darbo funkcijų, turi būti paskirtas kitas pavaduojantis asmuo. Užsakymų vykdymas ar gedimų šalinimas negali nutrūkti dėl kažkurio darbuotojo nebuvimo darbe.
2.3.	Gedimų registracija vykdoma per pasirinktą komunikavimo kanalą (Jira, Slack, el. paštas, kita). Tiekėjas ne vėliau nei kaip numatyti terminai turi reaguoti bei išspręsti užregistruotą gedimą. Išsprendimo terminas negali būti ilgesnis nei buvo numatytas, nebent dėl objektyvių priežasčių, susiderinus su Perkančiąją įstaiga, terminas bus pratęstas. Vienašališkai Tiekėjas negali pratęsti termino. Gedimų lygį (kritinė klaida, vidutinio svarbumo klaida, klaida) nurodo Perkančioji organizacija.
2.4.	Reakcijos (atsakymo) laikas po pranešimo apie gedimą: • Kritinės klaidos atveju (visa TVS ar atskiros jos dalys neveikia, URM svetainė ir/ar DA svetainės nepasiekiamos (-os) lankytojams) – ne ilgesnis kaip 2 val. darbo dienomis; • Vidutinės svarbos klaidos atveju (neveikia vienas ar keli TVS ar URM ir/ar DA svetainių moduliai/blokai, kitos dalys veikia korektiškai) - ne ilgesnis kaip 4 val. darbo dienomis; • Klaidos atveju (URM ir/ar DA svetainių veikimas neatitinka pirkimo sutartyje nustatytų reikalavimų, nedideli dizaino neatitikimai) – ne ilgesnis kaip 8 val. darbo dienomis.
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 16 val. darbo dienomis.
2.6.	Už paslaugas mokama pagal sutartyje nurodytą priežiūros paslaugų tiekimo valandinį įkainį.

Eil. Nr.	3. REIKALAVIMAI VYSTYMIUI
3.1.	Užsakymo naujam funkcionalumui pateikimas vykdomas per pasirinktą komunikavimo kanalą (Jira, Slack, el. paštas, kita). Tiekėjas 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 Perkančiąją įstaiga, terminas bus pratęstas. Vienašališkai Tiekėjas negali pratęsti termino.
3.2.	Už paslaugas mokama pagal sutartyje nurodytą vystymo paslaugų tiekimo valandinį įkainį.
3.3.	Tiekėjas nurodydamas sumą, turi įskaičiuoti visus mokesčius bei galimas papildomas išlaidas (mokamos nuotraukos, kita).
3.4.	Užsakovas turi matyti užsakymo statusą, praleistas valandas, turi turėti galimybę papildyti užsakymą, prisegti priedus, rašyti komentarus.
3.5.	Tiekėjas visus naujus funkcionalumus ar esamų patobulinimus turi talpinti testinėje svetainėje. Tik perkančiai organizacijai patvirtinus juos, bus galimas diegimas produkcinėje aplinkoje.
3.6.	URM svetainės ir šablono DA svetainėms vystymo paslaugos neturi sutrikdyti URM svetainės ir DA svetainių veikimo.
3.7.	Suteikus Svetainės vystymo paslaugas, Tiekėjas privalo atnaujinti dokumentaciją (administravimo vadovą, technologinę dokumentaciją (naudojamos TVS, duomenų bazių ir kitų komponentų aprašymai ir tarpusavio sąryšio bei išdėstymo schemas), diegimo ir konfigūravimo instrukcija) kurioje būtų išsamiai aprašytas realizuotas naujas funkcionalumas ir kita informacija. Dokumentacija turi būti parengta lietuvių kalba.
3.8.	Suteikus Svetainės vystymo paslaugas Perkančiajai organizacijai perduodami svetainės išeities kodai, kurie talpinami Perkančiosios organizacijos SVN saugykloje.

Eil. Nr.	4. APLINKOS APSAUGOS KRITERIJŲ TAIKYMAS
4.1.	Perkamos paslaugos atitinka 2011 m. birželio 28 d. Nr. D1-508 Lietuvos Respublikos Aplinkos ministro įsakymo „Dėl aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinimo“ 4.4.3. punkto nuostatas: perkama tik nematerialaus pobūdžio (intelektinė) ar kitokia paslauga, nesusijusi su materialaus objekto sukūrimu, kurios teikimo metu nėra numatomas reikšmingas neigiamas poveikis aplinkai, nesukuriamas taršos šaltinis ir negeneruojamos atliekos (programavimo, informacinių sistemų priežiūros paslaugos ir kitos paslaugos)

Eil. Nr.	5. REIKALAVIMAI SAUGUMUI
5.1.	Duomenų sauga turi būti užtikrinta remiantis asmens duomenų apsauga ir remiantis: • 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 (Bendrasis duomenų apsaugos reglamentu); • Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu; • Lietuvos Respublikos kibernetinio saugumo įstatymu; • 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“; • Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“; • 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: OWASP programinės įrangos saugos užtikrinimo standartu (angl. OWASP Application Security Verification Standard 4.0.1). OWASP Saugaus programavimo gairėmis (angl. OWASP SCP Quick Reference Guide v).
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
5.3.	Sistema turi užtikrinti veikimą naudojantis HTTPS saugiu protokolu.
5.4.	Jungiantis HTTP protokolu, naudotojas turi būti nukreipiamas į sistemą HTTPS protokolu.
5.5.	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.
5.6.	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.
5.7.	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.
5.8.	Serverio administravimo lygmenyje turi būti naudojama SSH (angl. Secure shell).
5.9.	Sistema turi būti apsaugota nuo: - Neautentifikuotos prieigos. - Nesankcionuoto naudotojo sesijos perėmimo. - Nesankcionuoto duomenų perėmimo ar jų įterpimo. - Nuo SQL injekcijų į duomenų bazę.
5.10.	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 .
5.11.	Duomenų bazėje turi būti naudojamos parametrizuotos SQL užklausos.
5.12.	Turi būti realizuotas sprendimas, leidžiantis administruoti TVS tik jungiantis iš nurodytų IP adresų ar jų režijų. Prisijungimai prie TVS sistemos turi būti fiksuojami ir saugomi (įskaitant ir nesėkmingus bandymus prisijungti).
5.13.	Turi būti uždrausta prieiga prie objektų, kurie atskleidžia perteklinę informaciją.
5.14.	Turi būti realizuotas informacijos kaupimas apie sistemos klaidas su galimybe jas peržiūrėti.
5.15.	Duomenų bazė turi būti suprojektuota pagal gerąsias duomenų bazių projektavimo praktikas.
5.16.	Turi būti realizuotos konfidencialumą užtikrinančios priemonės (turi būti užtikrintas slaptažodžių saugumas juos koduojant vienkpusio 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. plaint text), ar koduojant visuotinai pripažintais nesaugiais šifravimo algoritmais (pvz. MD5).
5.17.	Užsakovo iniciatyva atliekamas svetainės ir svetainėje naudojamų komponentų saugos testavimas. Identifikavus svetainėje naudojamo programinio kodo pažeidžiamumus, Tiekėjas privalo juos ištaisyti kuo skubiau, bet ne vėliau, kaip per 4 d. d. nuo šios informacijos gavimo datos. Jeigu šių spragų per numatytą laiką pašalinti nėra galimybės dėl pagrįstos priežasties, turi būti įgyvendintos laikinos spragų užkardymo arba poveikio sumažinimo priemonės.
5.18.	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;

	• naudojamas sertifikatas, išduotas patikimos organizacijos, draudžiama naudoti pasirašytus neautorizuotos šifrų pasirašymo sistemos (angl. self-signed) sertifikatus; • sertifikato rakto ilgis ne mažiau negu 2048 bitų ilgio; • prieiga prie privačių šifravimo raktų ribojama ir griežtai kontroliuojama. Privatūs šifravimo raktai saugomi kaip įmanoma mažesniame vietų skaičiuje – tarnybinėje stotyje, o atsarginė kopija – atsarginių kopijų tarnybinėje stotyje.
5.19.	Užsakovas turi teisę patikrinti svetainės atitiktį saugumo reikalavimams (atitikties vertinimas, įsilaužimų testavimas ir kt.). Nustačius neatitiktis paslaugų teikėjas įsipareigoja neatitiktis pašalinti.