VSTUPENKOVÝ A POKLADNÍ SYSTÉM PRO MUZEA A GALERIE

Specifikace předmětu plnění

Technické podmínky

I. Předmět plnění

1. Účelem veřejné zakázky je pořízení funkčního vstupenkového a pokladního systému (dále jen „Systém“) pro posílení hospodárného využití finančních prostředků, s rychlou implementací a se zárukou udržitelnosti, aktualizace a dalšího vývoje Systému.
2. Systém je určen pro komplexní správu vstupenek a prodej zboží na pokladně.
3. Systém je určen pro kulturní zařízení a instituce Kraje Vysočina, tj. zejm. tyto příspěvkové organizace Kraje Vysočina a jimi provozovaná muzea, galerie či knihovny:
    a. Muzeum Vysočiny Jihlava (dále jen „MVJ“), vč. všech poboček a odloučených pracovišť:
        - MVJ – muzeum Jihlava,
        - Hrad Roštejn, pobočka MVJ,
        - Muzeum Telč, pobočka MVJ,
        - Muzeum Třešť, pobočka MVJ,
    b. Oblastní galerie Vysočiny (dále jen „OGV“), vč. všech pracovišť:
        - Expoziční budova Komenského 10, Jihlava,
        - Expoziční budova Masarykovo nám. 24, Jihlava,
    c. Muzeum Vysočiny Pelhřimov (dále jen „MVP“), vč. všech poboček a odloučených pracovišť:
        - MVP – muzeum Pelhřimov,
        - Hrad Kámen, pobočka MVP,
    d. Horácká galerie v Novém Městě na Moravě,
    e. Krajská knihovny Vysočiny

    a v budoucnu případně další zřízené či založené, resp. další zřizované či zakládané organizace Kraje Vysočina

    (dále společně jen „subjekty“).
4. Systém bude naimplementován a provozován v privátním cloudovém prostředí Technologického centra Kraje Vysočina.
5. Systém je opatřen licencí bez omezení počtu zřizovaných či zakládaných organizací Kraje Vysočina, počtu pracovišť a počtu pověřených zaměstnanců těchto organizací a uživatelských stanic.
6. V případě rozhodnutí zadavatele o využití Systému dalšími zřizovanými či zakládanými organizacemi Kraje Vysočina, než jsou uvedeny ve výčtu v odst. 3. výše, je součástí předmětu plnění poskytování veškerých prací, činností, služeb a podpory pro zahájení jejich plnohodnotného užívání Systému, tj. zejména jejich zapojení do Systému, provedení veškerých nezbytných instalací Systému či jeho instancí, poskytnutí přístupových práv, zřízení účtů organizace, pracovišť či poboček, uživatelských účtů apod.
7. Součástí předmětu plnění je rovněž:
    - zprovoznění a nastavení Systému u každého subjektu dle odst. 3 písm. a) až e) tohoto oddílu,

- provedení odborných školení u každého subjektu dle odst. 3 písm. a) až e) tohoto oddílu, tj. zaškolení administrátorů – admin subjektu a pobočkový admin a zaškolení dalších uživatelů – pokladních (viz také oddíl III. níže), a to před zahájením užívání Systému subjektem, a dále při změnách Systému
- dále předání uživatelské dokumentace každému subjektu.

8. Součástí předmětu plnění je následná odborná podpora provozu a poskytování či provádění aktualizací, jak je podrobně upraveno v podmínkách servisní smlouvy.

II. Technické požadavky na Systém pro provoz v Technologickém centru Kraje Vysočina

III. Administrátorská oprávnění a správa vstupenek

IV. Ekonomická agenda

V. Správa prodeje vstupenek

VI. Správa skladů a prodeje zboží

VII. On-line rezervace a prodej vstupenek

VIII. Statistiky

Technické podmínky, které jsou předmětem oddílů II. až VIII. výše, jsou uvedeny v Technickém listu, který je součástí přílohy č. 1 Výzvy k podání nabídek – Specifikace předmětu plnění.

IX. Zabezpečení dat a Systému (Z)

Zadavatel/objednatel požaduje splnění následujících bezpečnostních požadavků:

- Systém zaznamenává auditní logy a umožňuje zástupcům zadavatele/objednatele přístup k těmto informacím, které musí zahrnovat všechny informace o úpravách všech uložených souborů a jejich metadat včetně informace, kdo se souborem manipuloval.
- Auditní záznamy a logy Systému musí obsahovat minimálně tyto informace:
    - přihlášení a odhlášení všech uživatelů (včetně administrátorů či jiných privilegovaných účtů),
    - činnosti provedené administrátory, např. (pokud danou funkcionalitu obsahují):
        - přidělení/odebrání oprávnění,
        - založení/smazání uživatele
        - přidělení/odebrání role
        - reset hesla (pokud je prováděn na úrovni logujícího informačního aktiva)
        - povýšení oprávnění administrátora, převzetí role konkrétního uživatele
        - změna konfigurace logování událostí
        - změna konfigurace informačního aktiva,
    - činnosti prováděné uživateli,
    - automatická informační, varovná a chybová hlášení provozního charakteru (tzv. aplikační logy).
- Systém musí zaznamenávat auditní záznamy a logy na všech existujících úrovních, tj. na úrovni:
    - operačního systému aplikačního serveru,
    - aplikačního serveru/modulu aktiva (např. web server, sql server, apod.),
    - samostatné aplikace/informačního systému/služby informačního systému.
- Systém podporuje a vynucuje přístup přes šifrované spojení prostřednictvím webového prohlížeče (HTTPS) pro přístup k veškerým uloženým informacím, přičemž nastavení TLS protokolu musí odpovídat níže uvedeným požadavkům na kryptografii.

- Aplikační servery/moduly (např. web server, DB server, apod.) systému nesmí vyžadovat pro své spuštění privilegovaná oprávnění (např. typu root, Administrator, NT Authority\System, apod.).
- Pokud jsou v systému použity nějaké kryptografické funkce a algoritmy, musí tyto funkce a algoritmy splňovat požadavky uvedené v příloze č. 1 tohoto technického zadání.
- Webové servery použité v systému musí být implementovány tak, aby byly splněny následující požadavky na HTTP hlavičky:
    - X-Frame-Options
        - Musí být implementována (tzn. server ji musí klientské aplikaci zasílat) – v odůvodněných případech může být vynechána.
        - Záhlaví může nabývat pouze hodnot DENY nebo SAMEORIGIN dle potřeby
    - Strict-Transport-Security
        - Musí být implementována
        - Direktiva max-age musí nabývat hodnoty minimálně 31536000
    - Content-Security-Policy
        - Musí být implementována
        - Nesmí obsahovat direktivy unsafe-inline, unsafe-eval
        - Aktiva mohou být načítána pouze prostřednictvím zabezpečeného protokolu (direktiva https:)
        - Aktiva mohou být načítána pouze z konkrétních a bezpečných zdrojů
        - Pokud by bylo nutné načítat aktiva z jiných zdrojů, které nejsou umístěny na infrastruktuře, která je v držení Kraje Vysočina nebo dodavatele, podléhají tyto zdroje nejprve schválení Krajem Vysočina. Pokud ke schválení Krajem Vysočina nedojde, tyto zdroje nemohou být použity k načítání aktiv spolu se zbytkem webové stránky
    - X-Content-Type-Options
        - Musí být implementována
    - Referrer-Policy
        - Musí být implementována
        - Nesmí obsahovat direktivy: prázdný string, unsafe-url
    - Permissions-Policy
        - Musí být implementována
        - Mohou být povolena pouze ta oprávnění, která jsou skutečně potřeba, všechna ostatní musí být explicitně zakázána
    - X-XSS-Protection
        - Musí být implementována
        - Directiva politiky musí nabývat hodnoty 1; mode=block
    - Server
        - Pokud je hlavička implementována, musí být změněna tak, aby neodhalovala citlivé informace odhalující verzi webového serveru
    - Set-Cookie
        - Pokud se jedná o session cookies, musí obsahovat direktivu nastavující secure a httponly flagy.
    - Cross-Origin-Embedder-Policy
        - Musí být implementována
    - Expect-CT
        - Musí být implementována
    - Cross-Origin-Opener-Policy
        - Musí být implementována

    - Cross-Origin-Resource-Policy
        - Musí být implementována
- K systému musí být dodána provozně bezpečnostní dokumentace v tomto rozsahu:
    - Instalace systému
    - Základní konfigurace
    - Záloha, obnova, restart
        - Strategie zálohování systému navržená dodavatelem
        - Zpracovaný disaster recovery plán, tedy posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému po jeho selhání do jeho plně funkčního stavu
            - Včetně potřebných zdrojů, jako je např. SW, HW, přístupové údaje, data, parametry disaster recovery prostředí, apod.
        - Posloupnost kroků (co a jak udělat), které je třeba provést pro bezpečné restartování systému tak, aby naběhl do původního stavu
    - Monitoring
        - Výčet a popis v šech událostí, které jsou zaznamenávány
        - Způsob uložení zalogovaných událostí
        - Návrh způsobu provozního monitoringu
    - Základní uživatelská a administrátorská příručka

X. Řízení přístupových oprávnění (O)

- Systém musí umožňovat práci se skupinami uživatelů a přiřazování oprávnění těmto uživatelům.
- Systém musí umožňovat přiřazování oprávnění na základě rolí (tyto role mohou být řešeny skupinami).
- Systém musí pro autentizaci vůči internímu zdroji identit:
    - umožnit nadefinování vlastní heslové politiky, a to minimálně v tomto rozsahu:
        - stáří hesla,
        - granulární komplexita hesla (určení kategorií znaků),
        - délka hesla,
        - historie hesla (počet opakování).
    - ukládat hesla v DB tak, aby byla v souladu s požadavky na kryptografii, tj. nesmí být uložena v plaintext podobě ani pomocí nevhodných hash funkcí.

XI. Kryptografie (K)

Pro šifrování, elektronické podepisování a provádění otisků dat (hashování) nesmí být použity proprietární/uzavřené algoritmy, ale ty, které jsou považovány za standardy, jejich funkcionalita je všeobecně známá.

Použité kryptografické prostředky (např. algoritmy, funkce, apod.) musí splňovat doporučení v oblasti kryptografických prostředků vydávaných Národním úřadem pro kybernetickou a informační bezpečnost v aktuálním znění na webových stránkách úřadu.

XII. Hardware (H)

Systém musí umožňovat použití čtečky vstupenek (jak vstupenek v listinné, tak v elektronické podobě) pro rychlejší odbavení většího počtu návštěvníků.

Dodávka HW není předmětem této veřejné zakázky. Dodavatel ve své nabídce uvede, jaký HW je pro práci s dodávaným SW vhodný či nezbytný, vč. případných specifických požadavků na něj. V případě, že dodavatel je rovněž dodavatelem takového HW, uvede ve své nabídce ceny, za které

takový HW nabízí. Jednotlivé subjekty si pak na základě svých potřeb u dodavatele takový HW případně objednají samostatně.

XIII. Akceptační testy

Po předání dokončeného plnění na základě smlouvy o dílo budou provedeny akceptační testy, a to v následujících oblastech a rozsahu (viz také podmínky smlouvy o dílo):

- vytvoření nového tenantu a adminů pro subjekt,
- přihlášení uživatele prostřednictvím krajské identity,
- vytvoření alespoň 1 vstupenky každého druhu dle Technického listu a její deaktivace,
- on-line rezervace vstupenky a její on-line prodej,
- správa prodeje vstupenek,
- funkčnost ekonomické agendy,
- funkčnost skladového hospodářství,
- generování datových sestav v rámci statistik,
- export dat za subjekt,
- prokázání splnění bezpečnostních požadavků.