Veřejná zakázka **Centrální systém evidence sbírkových předmětů**

Příloha č. 1 Zadávací dokumentace – **technické podmínky (textová část)**

**Centrální systém evidence sbírkových předmětů**

**Správa sbírek muzejní povahy Kraje Vysočina**

**Technická specifikace předmětu veřejné zakázky**

Centrální systém evidence sbírkových předmětů (dále jen Systém).

1. **Předmět plnění** 
   1. Záměr Příjemce je pořízení funkčního ***Systému* určeného pro evidenci sbírek muzejní povahy** z důvodu hospodárného využití finančních prostředků, rychlé implementace a **záruky vývoje Systému**.
   2. Dodávka Systém je určena pro **centrální evidenci sbírkových předmětů vlastněných Krajem Vysočina a spravovaných jím zřizovanými organizacemi**. Systém umožňuje evidenci všech typů sbírek muzejní povahy a všech evidovaných předmětů.
   3. **Systém je opatřen časově neomezenou licencí užívání**.
   4. Systém je opatřen **licencí bez omezení na počet sbírkotvorných organizací, evidovaných předmětů, sbírek** a **na počet pověřených zaměstnanců** těchto organizací a **uživatelských stanic**.
   5. Součástí dodávky je **schéma oborových školení** a zpracování uživatelské dokumentace.
   6. Součástí dodávky je **následná odborná podpora provozu** a **zajištění aktualizací**
2. **Obecné požadavky**
   * Systém respektuje české normy a zákony, vč. vyhlášek a prováděcích předpisů, a v době předání díla, tak i v průběhu následné podpory. Jedná se zejména o:
     1. zákon č. 122/2000 Sb., o ochraně sbírek muzejní povahy, ve znění pozdějších předpisů (změna: 186/2004 Sb., 483/2004 Sb., 203/2006 Sb.),
     2. zákon č. 303/2013 Sb., měnící zákon č. 122/2000 Sb.,
     3. vyhláška Ministerstva kultury, kterou se provádí zákon č. 122/2000 Sb., o ochraně sbírek muzejní povahy a o změně některých dalších zákonů,
     4. vyhláška č. 96/2013 Sb., kterou se mění vyhláška č. 275/2000 Sb., kterou se provádí zákon č. 122/2000 Sb., o ochraně sbírek muzejní povahy a o změně některých dalších zákonů,
     5. metodický pokyn Ministerstva kultury, č. j. 53/2001, k zajišťování správy, evidence a ochrany sbírek muzejní povahy v muzeích a galeriích zřizovaných Českou republikou nebo územními samosprávnými celky (kraji, obcemi),
     6. metodický pokyn Ministerstva kultury k evidenci a inventarizaci sbírkových předmětů a k doplnění obrazových údajů pro charakteristiku sbírky v CES a ke změně zákona č. 122/2000 Sb. zákonem č. 303/2013 Sb.,
     7. metodický pokyn Ministerstva kultury č. j. 16688/2014 k evidenci a inventarizaci sbírkových předmětů a k doplnění obrazových údajů pro charakteristiku sbírky v CES a ke změně zákona č. 122 Sb. zákonem č. 303/2013 Sb.,
     8. metodický pokyn k provedení vyhlášky MF č. 270/2010 Sb., o inventarizaci majetku a závazků.
   * Systém bude dodržovat správnost a průkaznost sbírkové evidence vedené v muzeích a galeriích zřizovaných krajem, režim zacházení se sbírkou a sbírkovými předměty.
   * Systém bude plně respektovat mezinárodní normy a doporučení, zejména CIDOC-CRM. (<https://www.cidoc-crm.org/>) (Nepovinný požadavek - R)
   * Systém bude využívat/poskytovat standardizované evropské protokoly, zejména OAI-PMH. (<https://www.openarchives.org/pmh/>) (Nepovinný požadavek - R)
   * Systém kompatibilní s digitalizací evropského kulturního dědictví a budoucí platformy Společný evropský cloud pro kulturní dědictví – European Collaborative Cloud for Cultural Heritage (ECCCH). (<https://pro.europeana.eu/post/europeana-initiative-responds-to-call-for-a-european-collaborative-cloud-for-cultural-heritage>)
   * Systém bude kompletně komunikovat v českém jazyce, dokumentace cílového řešení a provozní dokumentace (tj. uživatelské a administrátorské příručky) budou v českém jazyce.
3. **Požadavky na Systém v oblasti evidence sbírek: Obecné požadavky**
   * Systém umožňuje **uživatelské úpravy designu formulářů / masek** pro záznamy o sbírkovém předmětu pro jednotlivé sbírkové skupiny (fondy) a jejich specifika, včetně možnosti nastavení povinných a nepovinných hodnot
   * Systém umožňuje vytvoření nové sbírky nebo podsbírky nebo fondu, včetně její datové struktury a to pomocí nástrojů administrátora. Systém umožňuje libovolné přidávání či ubírání sbírek a podsbírek a fondů.
   * V rámci organizací kraje je evidována následující množina druhů podsbírek typicky s cca 50-100 atributy na podsbírku. Jedná se o tyto **druhy podsbírek** a součástí dodávky bude příprava jejich struktury (datového modelu a formulářové šablony):
     1. 1 – Geologická
     2. 2 – Petrografická
     3. 3 – Mineralogická
     4. 4 – Paleontologická
     5. 5 – Botanická
     6. 6 – Mykologická
     7. 7 – Entomologická
     8. 8 – Zoologická
     9. 9 – Archeologická
     10. 10 – Historická
     11. 11 – Etnografická
     12. 12 – Antropologická
     13. 13 – Numizmatická
     14. 14 – Militaria
     15. 15 – Výtvarného umění
     16. 16 – Uměleckého řemesla
     17. 17 – Uměleckoprůmyslové práce
     18. 18 – Knihy
     19. 19 – Písemnosti a tisky
     20. 20 – Negativy a diapozitivy
     21. 21 – Fotografie, filmy, videozáznamy a jiná média
     22. 22 – Přenesené historické stavby (skanzeny)
     23. 23 – Věda, technika a průmyslová výroba
     24. 24 – Další
     25. 25 – Ostatní
   * Systém umožňuje **automatizovaný proces převodu dat z chronologické do systematické evidence**.
   * Systém podporuje **práci se slovníky** (standardizace, zabránění chybných popisů, mezinárodní slovníky, jména osobností, místních jmen, biologická taxonomie apod.). Systém obsahuje odborné slovníky a včetně mechanismu jejich aktualizace:
     1. Číselník územního členění až do úrovně adresního místa - RUIAN ČUZK – aktualizace jednou za 3 měsíce
     2. Geomorfologické členění ČR – CENIA – 1x ročně
     3. Biogeografické členění ČR - CENIA – 1x ročně
     4. Fytogeografické členění ČR - CENIA – 1x ročně
   * Jednotné krajské číselníky s centrální správou (samostatné uživatelská role správce per číselník) - autoři, materiály, techniky. Včetně možnosti tvorby uživatelských číselníků a slovníky – možnost uživatelem (krajským správcem) definovaného číselníku nebo slovníku (např. biologická taxonomie).
   * Podpora hierarchických slovníků (např. biologická taxonomie)
   * Možnost importu jednorozměrných i hierarchických číselníků a slovníku z XLSX (dle definované šablony)
   * Systém **obsahuje jednotnou a jednoznačnou dataci** (časovou osu), uložení datace číslem i názvem. Systém pracuje s nabídkovými listy datace (zabránění duplikací, přehledná sestava datací), resp. naformátování možností datace tak, aby nedocházelo k chybám v zápisu. Předpokládá se pro každý sbírkový předmět uvedení:
     1. číselník: datace od – do (konkrétní letopočet),
     2. číselník: možnost identifikace období (např. gotika, baroko, renesance, Druhá světová válka apod.) / umělecký styl apod.,
     3. textová pole: Další kurátorské specifikace v dataci (14. března 1836, odpoledne, když pršelo… apod.)
   * Systém umožňuje **hromadné operace s daty**, minimálně v rozsahu:
     1. hromadný záznam o inventuře možnost provést hromadně záznam o jejím provedení apod.
     2. hromadné nahrazení textu v poli
     3. hromadné doplnění údaje pro skupinu (rozsah) inventárních čísel nebo jinak vyfiltrovaných záznamů
   * Systém umožňuje **evidenci multimédií a další dokumentace**: existuje možnost přikládat a strukturovaně ukládat neomezené množství souborů (obrázky, videa, zvuk, textové dokumenty apod.). **Dokumenty lze vkládat přes webové rozhraní** systému ale **také dávkou v podobě nahrání souborů** obsahujícího větší počet multimédií a dokumentů na server – *Systém* si fotky přiřazuje k jednotlivým evidovaným položkám sám.
   * Poskytovatel vytvoří metodiku a prostředí pro dávkový import multimediálních příloh (včetně správného přiřazení k jednotlivým předmětům).
   * Systém umožňuje **evidenci související dokumentace** (pořizovací doklady, nálezové a restaurátorské zprávy apod.). Systém definuje akceptovatelné formáty příloh.
   * Systém podporuje **automatizované procesy** - systém povede uživatele definovanou posloupností kroků. Příklad - nabývání předmětů do sbírky, logicky za sebou řazené formuláře:

**I. formulář** – výběr druhu nabytí, vyplnění povinných hodnot, připojení příloh:

* + - 1. vlastním sběrem (volitelné přílohy)
      2. darem od fyzických či právnických osob, případně převodem od právnických osob či dědictvím od fyzických osob (povinná darovací smlouva jako příloha, volitelná příloha protokol k doprovodné dokumentaci)
      3. koupí od fyzických či právnických osob (povinná kupní smlouva)

**II. formulář** – podklady pro poradní sbor - jen v případě nabytí kupní smlouvou (povinné přílohy): nabídkový list, návrh kurátora, protokol z jednání poradního sboru

**III. formulář** – přidělení přírůstkového čísla (ve formě: Ji-1/2024, zápis do přírůstkové knihy)

* + V závislosti na definovaných oprávněních Systém umožňuje **fulltextové vyhledávání** včetně všech vedlejších tabulek a přiložených dokumentů, které jsou opatřeny textovou vrstvou. Je umožněno parametrické vyhledávání přes celý Systém napříč všemi daty včetně vedlejších tabulek a přiložených dokumentů (minimálně formát PDF a DOCX) na základě zadaných kritérií (vč. funkcí vyhledávání typu „starší/mladší než“ a „je ve vybraném časovém intervalu“ včetně datace historických období (baroko, gotika, paleolit) na příkladu: 1. 1. 1939 - 31. 12. 1945).
  + Systém podporuje snadné **řazení, vyhledávání a filtrování, včetně sestav** (filtrování, vyhledávání a třídění karet v přehledu podle jednotlivých údajů na kartě - podle podsbírky, evidenčního čísla, podle uložení, tj. např. lokační seznamy depozitářů, názvu autora, techniky, materiálu apod.) Systém umožňuje seřazení podle vybraného údaje i v tiskových sestavách.
  + Systém umožňuje **ukládání uživatelských filtrů a nastavení**. Je zajištěna podpora, přizpůsobení a uložení uživatelského prostředí, včetně zobrazovacích profilů. (Nepovinný požadavek - R)
  + Systém je vybaven **kontextovou nápovědou**.
  + Je umožněn snadný přístup ke **všem agendám Systému** ve vztahu k danému předmětu (evidence, manipulace, inventarizace, depozitář, publikace, restaurování apod.) a slovníky. Tj. je zajištěno vzájemné aplikační propojení mezi jednotlivými agendami – z jednoho místa lze získat veškeré informace o sbírkovém předmětu (příklad: při prohlížení karty lze např. proklikem zjistit, zda předmět právě není restaurován, příp. dopracovat se k předešlým restaurátorským zprávám, tj. kurátor nemusí pro zjištění informací o restaurování spouštět samostatný modul pro restaurování a v něm daný předmět dohledávat apod.).
  + Systém umožňuje **sestavení kolekcí předmětů**, tj. skupiny obecně nesouvisejících předmětů sestavených kurátory průřezově ze všech podsbírek a ze všech paměťových institucí KV s možností publikace pro veřejnost.
  + Nástroj pro publikaci kolekcí pro veřejnost umožňuje vytvoření samostatné veřejné prezentace na samostatném DNS typu sbirky.kr-vysocina.cz s rozcestníkem na jednotlivé kolekce (každá kolekce má své jednoznačné URL). U každé kolekce je možné definovat samostatný grafický design ve smyslu barev, fontů, loga organizace a doprovodných obrázků a textu. Součástí nástroje je samostatný prostor sumarizující kolekce dané instituce opět s možností samostatného designu (opět s možností jednoznačného URL).
  + Systém umožňuje **libovolné přidávání či ubírání paměťových institucí Kraje Vysočina včetně možnosti sloučení**.
  + Systém obsahuje **informace ohledně autorských práv ke sbírkovému předmětu**: možnost označení volného díla, licencovaného díla nebo chybějící vypořádání autorských práv apod. Systém **umožňuje přiřazení autorských práv**, podmínek užití (přiložení dokumentu Smlouvy na reprodukční práva k publikaci, smlouva týkající se pořízení sb. předmětu), včetně exspirace práv a implementace vodoznaku do obrázku (JPEG a JPEG2000) určeného ke zveřejnění.
  + Systém obsahuje **funkce statistiky** inventárních čísel a dalších čísel, počtu kusů předmětů v chronologické a systematické evidenci, počtu digitalizovaných předmětů, počtu vložených obrazových příloh, počtu evidenčních čísel, počtu vyřazených předmětů atd.

1. **Požadavky na Systém v oblasti evidence sbírek: Chronologická evidence**
   * Systém **umožňuje vést přírůstkovou knihu per sbírka,**, **generovat tiskové sestavy** přírůstkové knihy, **možnost uživatelských filtrů** podle vybraných parametrů.
   * Emailová notifikace kurátora o blížícím se termínu nutného převedení objektu do systematické evidence
2. **Požadavky na Systém v oblasti evidence sbírek: Systematická evidence**
   * Systém obsahuje:
     1. **kontrolu zápisu a možnost generování inventárních čísel** – zabránění duplicity, kontrola formátu
     2. **možnost nastavení formátu zápisu inventárního čísla**,
     3. **umožnění přiřadit jednomu přírůstkovému číslu více inventárních čísel** (v rámci každého sbírkového fondu).
     4. **Možnost vedení samostatné řady evidenčních čísel (**např. @ABC123 za účelem např. doprovodné evidence nebo biologických pozorování**)**
   * Systém umožňuje **hromadnou evidenci** (jedno inventární číslo může obsahovat více položek/kusů).
   * Systém umožňuje:
     1. **vkládání a správu faunistických a floristických dat** (pozorování bez inventárního čísla),
     2. **tvorbu terénních protokolů**,
     3. **práci se škrtacími seznamy terénních nálezů** (možnost vlastní konfigurace a ukládání záznamů),
     4. **tvorbu seznamů z lokalit**.
   * Systém umožňuje **doplnit záznamy o původu a historii předmětu, včetně lokace** (tj. existuje samostatný editovatelný záznam, který lze propojit s jiným záznamem), např. současná lokace s možností doplnění historické lokalit (+ např. fotky z lokality).
   * Možnost zadávání souřadnic ve formátu WGS84 (x,y,z)
   * Systém **umožňuje práci s daty GIS**, tj. načítání a editace nebo výběr dat z dodaného mapového webového klienta (souřadnice, katastry, nadmořský výška; podkladové mapy fytogeografické okresy, geomorfologické členění, územní členění dle RUIAN, ortofoto kraje, základní mapa CUZK). Včetně možnosti importu prostorových dat (minimálně formát SHP). Možnost vkládat externí data formou WMS a WMTS služeb.
   * Systém umožňuje vedení záznamů o **historických inventárních číslech** (např. po přečíslování).
   * Systém umožňuje **editaci uložených záznamů s uložením a vizualizací historie změn**.
3. **Požadavky na Systém v oblasti evidence sbírek: Akvizice**
   * Systém obsahuje **kompletní záznam akvizice** (univerzální šablony k vyplnění údajů s možností individuální úpravy, uložení a vytváření nových a dále používaných šablon).
   * Systém umožňuje **editaci šablon smluv** pro institucionální úpravu (hlavičky apod.).
   * Systém umožňuje **propojení (zobrazení) zapsaných údajů** mezi jednotlivými evidencemi (např. evidence I. a II. stupně, přírůstkového čísla a údaje o akvizici).
4. **Požadavky na Systém v oblasti evidence sbírek: Manipulace se sbírkovými předměty**
   * Systém obsahuje agendu **uložení sbírkových předmětů** a **manipulace se sbírkovými předměty** (lokační seznamy v depozitáři, výpůjčky, výstavy, přemísťování, badatelská činnost vč. variantních výpůjčních smluv (s uvedením pojišťovací ceny a náhledu na dřívější ceny) s možností editace a vytváření šablon.
   * Systém **generuje a eviduje výpůjční a zápůjční smlouvy** s možností jejich editace a vytváření šablon a možností odkazu na finální smlouvu (URL) na externí úložiště smluv.
   * Systém umožňuje nastavení **upozornění kurátora emailem na blížící se konec lhůty výpůjčky i zápůjčky**.
   * Systém obsahuje **evidenci historie pohybu sbírkových předmětu**.
   * **V rámci propojení s CES Systém obsahuje možnost aktualizace, včetně povolování dočasných vývozů sbírkových předmětů, rozhodnutí rady kraje o souhlasu/vzetí na vědomí s dočasným vývozem sbírkových předmětu** (číslo usnesení).
   * Systém je **schopen přiřazení přílohy výpůjčních smluv** (na základě výběru ze seznamu standardních příloh).
   * Systém generuje, eviduje a archivuje **badatelské listy** a sestavuje základní statistky.
5. **Požadavky na Systém v oblasti evidence sbírek: Inventarizace**
   * Systém generuje **inventarizační seznamy** evidenčních čísel inventarizovaných předmětů, resp. existuje možnost vygenerování sestavy předmětů určených k inventarizaci (zachycení data inventarizace v systému a možnost generovat sestavy podle tohoto data).
   * Systém **zaznamenává pravidelné/mimořádné inventarizace** dle zákona.
   * Systém **obsahuje filtr nebo funkce o záznamech pravidelné inventarizace**, která poskytne informaci o předmětech, které dosud nebyly v rámci povinného cyklu inventarizovány, tj. obsahuje historii provedených inventarizací.
   * Systém **generuje tiskovou sestavu protokolů o provedení inventarizace**, vč. související zákonné agendy.
   * Systém umožňuje vést **záznam o stavu předmětu při inventarizaci**.
   * Řešení pro elektronickou inventuru – mobilní klient/zařízení pro provedení inventury, náhled na předmět s možností změny údajů, hromadný import/export dat pro inventuru
   * Emailová notifikace kurátora o blížícím se termínu nutného provedení inventury daného objektu v daném termínu
6. **Požadavky na Systém v oblasti evidence sbírek: Vyřazování sbírkových předmětů**
   * Systém obsahuje **nástroj pro návrh na vyřazení** Obsahuje zejména: důvod vyřazení, zápis z jednání sbírkotvorné komise, rozhodnutí Rady kraje o vyřazení sbírkového předmětu (číslo usnesení), datum vyřazení, doklad o vyřazení, poznámka k vyřazen (např. likvidace, nabídka, převod), nový majitel, hlášení do CES (pokud možno automatické).
7. **Požadavky na Systém v oblasti evidence sbírek: Evidence konzervátorsko-restaurátorských zásahů**
   * Systém **eviduje historii konzervátorsko-restaurátorských zásahů** k jednotlivým sbírkovým předmětům: datum a údaje o tom, kdo provedl zásah, příp. další doplňující informace.
   * Systém umožňuje **vkládání restaurátorských zpráv** a práci s nimi (vyhledávání, řazení apod.)
8. **Požadavky na vazby Systému**
   * Systém umožňuje **elektronickou komunikaci se systémem Centrální evidence sbírek** (CES). Zejména jde o nástroje pro podávání el. hlášení a předávání metadat o sbírkových předmětech.
   * Systém zajistí online **export / harvesting dat na portály eSbirky.cz** a **Europeana.eu** pomocí standardizovaných protokolů OAI-PMH.
   * Systém zajistí **exportní dávku pro informační systém Portálu systému evidence uměleckých děl** v případě ztráty předmětu(ů) provozované Policií ČR.
   * **Export metadat pro publikaci v systémech Digitální knihovna Vysočiny** (načítání dat katalogu do metadatového systému ProArc za účelem popisů v procesu digitalizace) (Nepovinný požadavek - R)
   * Integrace na **Registr sbírek výtvarného umění** (CITEM-PROMUS)
   * Číselníky muzejních autorit (CITEM)
9. **Manažerský modul**
   * Systému umožňuje řídit a kontrolovat práci správců/kurátorů sbírek zástupcem vlastníka sbírek, tj. vytvářet přehledy práce se Systémem, zejména v oblasti doplňování popisů a dat ke konkrétním sbírkovým předmětům v průběhu určitého časového období.

1. **Technická specifika**
   * Systém ukládá data automaticky (např. v rozpracovaných formulářích) v uživatelem nastaveném časovém intervalu. (Nepovinný požadavek - R)
   * Systém **zamezuje mazání metadat i multimediálních příloh na aplikační úrovni** (při potřebě mazání pouze označení objektu jako neaktivní) – to kvůli zachování reference master kopie do metadat.
   * Systém pracuje s **uživatelskými oprávněními**:
     1. přístupová práva na **jednotlivé úlohy (agendy) a funkce systému**,
     2. možnost nastavit **oprávnění na vybranou množinu dat** (např. na množinu dat, inventární řadu, podsbírku nebo od čísla po číslo apod.),
     3. **možnost kurátorského nastavení viditelnosti** **a přístupnosti** vybraných kurátorem spravovaných dat (např. pro kurátory, pro badatele, pro zástupce vlastníka, pro kurátory z ostatních paměťových institucí, pro veřejnost), tj. možnost omezení přístupu/zobrazení úplných informací.
   * **Systém podporuje UNICODE znakové sady**.
   * V rámci systému funguje **podpora kopírování záznamů** v Systému, výběr zdrojové karty a provedení kopie do nové karty.
   * Systém podporuje **export dat** (html, pdf, xls, xml). Systém je schopen exportovat jednotlivě uložené předměty (evidenční karty) jak v datové formě (struktura bude zdokumentována), tak v tištěné podobě (pdf).
   * Systém obsahuje **podporu tiskových výstupů** (možnost přednastavení a úpravy tiskové sestavy do formátu A4, A5 včetně možnosti volby tisku s obrázkem nebo bez obrázku).
   * Systém generuje a **umožňuje tisknout a načítá čárové kódy a QR kódy inventárních čísel**.
   * Systém je schopen **exportovat dávkově uložené předměty** v datové formě xml a xls (struktura bude popsána). Dávka bude definována jako:
     1. všechny předměty,
     2. výběr dle podsbírky,
     3. dle data (od-do),
     4. dle aktuálního filtru záznamů,
     5. možnost volby atributů pro export (např. selektivní vyjmutí velkých příloh z exportu).
2. **Požadavky na bezpečnost Systému** 
   * **Systém ukládá kompletní historii změn v Systému** (log list), a to minimálně v tomto rozsahu:
     1. Auditní záznamy a logy Systému musí obsahovat minimálně tyto informace:
        1. přihlášení a odhlášení všech uživatelů (včetně administrátorů či jiných privilegovaných účtů),
        2. činnosti provedené administrátory, např. (pokud danou funkcionalitu obsahují):
           1. přidělení/odebrání oprávnění,
           2. založení/smazání uživatele
           3. přidělení/odebrání role
           4. reset hesla (pokud je prováděn na úrovni logujícího informačního aktiva)
           5. povýšení oprávnění administrátora, převzetí role konkrétního uživatele
           6. změna konfigurace logování událostí
           7. změna konfigurace informačního aktiva,
        3. činnosti prováděné uživateli,
        4. automatická informační, varovná a chybová hlášení provozního charakteru (tzv. aplikační logy).
     2. Systém musí zaznamenávat auditní záznamy a logy na všech existujících úrovních – tj. na úrovni:
        1. operačního systému aktiva,
        2. aplikačního serveru/modulu aktiva (např. web server, sql server, apod.)
        3. samostatné aplikace/informačního systému/služby informačního systému.
   * **Formát (resp. standard) logů musí být v jedné z následujících možností, a to za účelem integrace na nástroj typu SIEM/log management:** 
     1. syslog (RFC 5424) + syslog over TLS,
     2. MS Windows Event Log (vlastní umístění XPath pro informační aktivum),
     3. W3C (pro MS IIS Web server),
     4. Standardní apache web server logy,
     5. SQL view,
     6. MS SQL audit logy,
     7. jiné (pouze na základě domluvy a po předchozím schválení zadavatele), např.:
        1. json,
        2. plain-text line-oriented logy,
        3. xml,
        4. atd.
   * Systém musí podporovat autentizaci vůči SSO Kraje Vysočina, která je založena na protokolu SAML2.0 a technologii Shibboleth.
   * Systém musí podporovat autentizaci vůči internímu zdroji identit pro tzv. fall-back přihlášení v případě nefunkčnosti SSO KV autentizace. Tento autentizační mechanizmus musí splňovat následující požadavky:
     1. Uložení hesel v interní databázi musí být zabezpečeno pomocí jedné z následujících bezpečných kryptografických funkcí:
        1. Argon2 s parametry alespoň t=1, m=221, p=4 a funkcí Argon2id
        2. scrypt s parametry alespoň N=32768 (215), r=8, a p=1
        3. PBKDF2 s počtem iterací alespoň 100 000 a hašovací funkcí SHA-2 (alespoň 256bit)
   * Pokud bude součástí systému webový server a webová aplikace, musí být tyto komponenty nastaveny tak, aby splňovaly tyto požadavky na bezpečnou komunikaci:
     1. SSL/TLS
        1. Podpora verzí protokolu TLS1.2 a TLS 1.3 (starší verze musí být zakázány)
        2. Ciphersuites použití v TLS protokolu musí podporovat Perfect forward secrecy a AEAD
     2. HTTP Headers – musí být aplikovány minimálně tyto bezpečnostní HTTP hlavičky:
        1. X-Frame-Options
           1. Záhlaví může nabývat pouze hodnot DENY nebo SAMEORIGIN dle potřeby
        2. Strict-Transport-Security
           1. Musí být implementována
           2. Direktiva max-age musí nabývat hodnoty minimálně 31536000
           3. Ostatní direktivy jsou volitelné
        3. Content-Security-Policy
           1. Musí být implementována
           2. Nesmí obsahovat direktivy unsafe-inline, unsafe-eval
           3. Aktiva mohou být načítána pouze prostřednictvím zabezpečeného protokolu (direktiva https:)
           4. Aktiva mohou být načítána pouze z konkrétních a bezpečných zdrojů
           5. 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 zbytek webové stránky
        4. X-Content-Type-Options
           1. Musí být implementována
        5. Referrer-Policy
           1. Musí být implementována
           2. Nesmí obsahovat direktivy: prázdný string, unsafe-url
        6. Permissions-Policy
           1. Musí být implementována
           2. Mohou být povolena pouze ta oprávnění, která jsou skutečně potřeba, všechna ostatní musí být explicitně zakázána
        7. X-XSS-Protection
           1. Musí být implementována
           2. Directiva politiky musí nabývat hodnoty 1; mode=block
        8. Server
           1. Pokud je hlavička implementována, musí být změněna tak, aby neodhalovala citlivé informace odhalující verzi webového serveru
        9. Set-Cookie
           1. Pokud se jedná o session cookies, musí obsahovat direktivu nastavující secure a httponly flagy.
        10. Cross-Origin-Embedder-Policy
            1. Musí být implementována
        11. Expect-CT
            1. Musí být implementována
        12. Cross-Origin-Opener-Policy
            1. Musí být implementována
        13. Cross-Origin-Resource-Policy
            1. Musí být implementována
3. **Ostatní požadavky**
   * V případě pochybností hodnotící komise v naplnění Technické specifikace Poskytovatelem si Příjemce vyhrazuje právo **požadovat od Poskytovatele funkční DEMO** pro ověření funkčností.
   * • Poskytovatel zajistí migraci všech dat těchto tří sbírek Kraje Vysočina z IS DEMUS (názvy dle Centrální evidence sbírek muzejní povahy): Sbírka Oblastní galerie Vysočiny v Jihlavě – kód sbírky GVJ/001-06-25/008001, Sbírka Horácké galerie v Novém Městě na Moravě – kód sbírky GHO/001-06-21/005001, Sbírka Galerie výtvarného umění v Havlíčkově Brodě – kód sbírky GHB/002-04-30/112002.
   * Systém definuje pravidla pro **dávkový import** dat z IS DEMUS, IS Bach a ze souborů Excel, Access ze všech paměťových institucí do příslušných odborných agend.
   * Součástí dodávky díla je školení v rozsahu
     1. Školení kurátorů po skupinách dle povahy sbírek (cca 3x6 hodin)
     2. Školení administrátorů systémů (cca 3 hodiny)
     3. Školení pro zástupce vlastníka sbírky (pracovníky kraje, cca 3 hodiny)
   * Součástí servisu jsou dále ad-hoc školení objednávaná na základě vysoutěžené ceny hodiny školení

**Technologické požadavky:**

|  |  |  |
| --- | --- | --- |
| **Požadavky - zkrácený text** | **Kód požadavku** | **Popis požadavku** |
| **Autentizace SSO KV** | **N01** | Pro ověření uživatele (autentizaci) je vyžadována integrace ASW na nástroje ověřování SSO KV = autentizační brána Authgate od firmy Autocont (AC Identita), která spravuje federaci Idp viz VysocinaID https://vysocinaid.kr-vysocina.cz. Ověřovací prostředí KV poskytuje službu autentizační brány (protokoly SAML2), kde služba centrálně ověřuje uživatele proti identitním prostorům spravovaným KV (AD, lokální účty IDM atd.) Na bránu SSO KV se nasměruje uživatelské přihlášení prostřednictvím https a výsledek ověření SSO KV vrátí ASW. Pokud systém poskytuje odkazy na své konkrétní objekty z externího prostředí (typicky link v emailové notifikaci) je nutné zabezpečit automatické směřování uživatele na tento objekt i v případě nutnosti přihlášení uživatele. |
| **Autorizace IDM** | **N02** | ASW si synchronizuje data přes API IDM AC Identita. Pro získání oprávněn uživatelů ASW (autorizace) je provedena autorizace proti databází uživatelských oprávnění na identity management KV (IDM). Databáze uživatelských oprávnění má vystaveno uživatelské rozhraní (API) ve formě web služeb SOAP (WS). ASW získává profil daného uživatele včetně oprávnění (rolí) prostřednictvím API na IDM KV, ukládá tyto parametry do svého interního nástroje správy uživatelů a v proceduře autorizace přiděluje na základě úspěšné autorizace příslušná oprávnění. |
| **Aplikační firewall BIG IP F5** | **N03** | ASW musí být plně funkční přes napojení na aplikační firewall BIG IP F5 tzn. aplikace musí být schopná plného fungování za aplikačním firewallem, který odděluje uživatele od aplikace a to včetně inspekce HTTPS provozu |
| **Systém ukládá kompletní historii změn v Systému** | **N04** | Systém musí v klíčových operacích s daty (vložení, editace, mazání) být schopen evidovat bez časového omezení stav dat před příslušnou operací s možností náhledu na data před danou změnou případně v daném časovém řezu. |
| **Formát (resp. standard) logů musí být v úvedených možnostech, a to za účelem integrace na nástroj typu SIEM/log management** | **N05** | ASW musí být schopen předávat vydefinované logy do SIEM nástroje, a to prostřednictvím alespoň jednoho z následujících protokolů/standardů:   * syslog (RFC 5424), * MS Windows Event Log (vlastní umístění XPath pro informační aktivum), * W3C (pro MS IIS Web server), * Standardní apache web server logy, * SQL view, * MS SQL audit logy, * jiné (pouze na základě domluvy a po předchozím schválení), např.:   + json,   + plain-text line-oriented logy,   + xml |
| **Systém musí podporovat autentizaci vůči internímu zdroji identit pro tzv. fall-back přihlášení v případě nefunkčnosti SSO KV autentizace** | **N06** | Systém musí podporovat scénář přihlášení klíčových uživatelů (správců) i v případě nefunkčnosti SSO a IDM s možností tvorby dalších lokálních účtů. |
| **Uložení hesel v interní databázi musí být zabezpečeno pomocí jedné z uvedených bezpečných kryptografických funkcí** | **N07** | Pro ukládání hesel uživatelů mohou být použity pouze tyto tzv. pomalé hashovací funkce:  • Argon2 s parametry alespoň t=1, m=221, p=4 a funkcí Argon2id  • scrypt s parametry alespoň N=32768 (215), r=8, a p=1  • PBKDF2 s počtem iterací alespoň 100 000 a schválenou hašovací funkcí SHA-2 (viz níže)  • při hashování hesla musí být použit pseudonáhodně vygenerovaný kryptografický salt  • pro ukládání hesel nesmí být použity tzv. rychlé hashovací funkce typu MD-X, SHA-X, apod. |
| **Systém podporuje bezpečné TLS protokoly a bezpečné ciphersuites** | **N08** | * verze protokolu minimálně TLSv1.2 a vyšší * konfigurace   + cipher suite musí být vybrána na základě serverem preferovaného pořadí   + vyšší priority musí mít cipher suites, které obsahují varianty asymetrických algoritmů s eliptickými křivkami, např.:     - ECDHE musí mít vyšší prioritu než DHE     - ECDSA musí mít vyšší prioritu než DSA   + všechny EXPORT cipher suites musí být zakázány   + algoritmy a funkce pro výměnu klíčů     - algoritmus pro výměnu klíčů musí podporovat Perfect forward secrecy       * tzn., že šifrovací klíč je vyměněn mezi klientem a serverem tak, aby jej nebylo možné získat se znalostí privátního klíče serveru, např. musí být použit Diffie-Hellman (DH nebo ECDH) algoritmus       * a navíc se musí jednat o tzv. ephemeral Diffie-Hellman (DHE, ECDHE), tzn. že pro každou session je generován nový set Diffie-Hellman klíčů     - délky klíčů:       * pro Diffie-Hellman (DH) - 3072 bitů       * pro Elliptic Curve Diffie-Hellman (ECDH) – 256 bitů a více     - nesmí být použita anonymní výměna klíčů   + algoritmy a funkce pro autentizaci     - minimální délky klíčů:       * RSA - 3072 bitů       * DSA – 3072 bitů       * ECDSA - 256 bitů   + algoritmy a funkce pro symetrické šifrování     - nesmí být použita hodnota NULL v cipher suites     - nesmí být použity tyto šifry:       * DES, 3DES, RC4     - minimální délka šifrovacího klíče - 128 bitů     - cipher suites s šiframi s větší délkou klíče musí mít větší prioritu v seznamu ciphersuites než s menší délkou klíče   + MAC (Message Authentication Code)     - použití SHA funkce s minimální délkou hashe 256 bitů     - vyšší délky otisků musí mít vyšší prioritu v cipher suites     **TLS cipher suites**   * Doporučené cipher suites (v doporučeném pořadí), které naplňují výše zmíněné požadavky * TLS1.3:   TLS\_AES\_256\_GCM\_SHA384  TLS\_CHACHA20\_POLY1305\_SHA256  TLS\_AES\_128\_GCM\_SHA256  TLS\_AES\_128\_CCM\_SHA256   * TLS1.2:   TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384  TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256  TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256  TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256  TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  TLS\_DHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 |
| **Systém podporuje všechny požadované bezpečnostní HTTP hlavičky** | **N09** | HTTP Strict Transport Security (HSTS)  X-Frame-Options (XFO)  X-Content-Type-Options  Content Security Policy (CSP)  Upgrade-Insecure-Requests. |
| **Platforma VMWARE** | **N10** | ASW je plně provozuschopný na serverové virtualizační platformě VMWare. |
| **Windows 2019 a vyšší** | **N11** | Preferovaný podporovaný operační systém pro provoz ASW je MS Windows Server 2019 nebo vyšší. V případě, že bude řešení dodáno na jiném OS, musí být servis OS (včetně záplatování a upgrade) součástí servisních služeb dodavatele |
| **MSSQL 2016 a vyšší** | **N12** | Preferované provozní databáze ASW jsou MS SQL Server 2016 a vyšší; V případě, že bude řešení dodáno na jiném databázovém systémů, musí být servis databázového systému (včetně záplatování a upgrade) součástí servisních služeb dodavatele |
| **Webová aplikace bez dalších komponent** | **N13** | Z hlediska technologie ASW jsou požadované webové aplikace typu lehký klient, umožňující pracovat bez instalace jakýchkoli dodatečných doplňků, komponent na koncové stanice jednotlivých uživatelů (např. Active X, Flash apod.) |
| **Prohlížeče (Edge, Chrome, Firefox) a platformy (Win, Lin, Andr, Mac)** | **N14** | ASW je navržen tak, aby byla funkční pro všechny běžné prohlížeče (Edge, Chrome a Firefox) bez omezení klíčové funkčnosti. Běžně lze zobrazit v aktuálních verzích prohlížečů na platformách Windows, Linux, Android, Mac OS X i iOS. |
| **Responsivní rozhraní (web+mobil)** | **N15** | Webové rozhraní je uzpůsobeno optimálnímu zobrazení a obsluze na různých technických zařízeních – osobní počítače, tablety, smartphone (responsivní rozhraní) |
| **Zákl. funkcionalita na mob. zařízení** | **N16** | Základní funkčnost ASW je dostupná i na mobilních zařízeních |
| **Správa uživatelů, oprávnění a rolí** | **N17** | ASW obsahuje nástroj pro správu uživatelů a uživatelských oprávnění na bází typizovaných rolí. |
| **Superadmin role s možností notifikací uživatelům s možnost přihlásit se na uživatele (pod jeho právy)** | **N18** | ASW umožní pro roli superadmina následující funkčnost: - zadávání notifikací s povinností potvrzení uživatele (pro všechny uživatele např. info o odstávce, nových funkcionalitách celého řešení, centrální podpory apod.) - přístup do dat všech organizací (tenatů) včetně možnosti přihlásit se v zástupu za uživatele jakékoliv organizace (tento stav přihlášení za jiného uživatele logovat/historizovat) |
| **Tvorba uživatelských reportů a statistik bez programování** | **N19** | ASW podporuje tvorbu statistik a reportů na úrovni uživatelského rozhraní a příslušné uživatelské role bez nutnosti programování |
| **Bezp. protokoly (HTTPS, SFTP, SSL)** | **N20** | ASW je navržen tak aby primárně podporoval protokoly zabezpečené komunikace (např. TLS, HTTPS, SFTP apod.) , které splňují níže uvedené bezpečnostní požadavky na kryptografii. |
| **Multitenantnost a jednotná adm. správa (superadmin)** | **N21** | ASW podporuje multitenantní architektur - tj. schopnost sdílet stejnou aplikaci a/nebo výpočetní zdroje více uživatelskými subjekty ve vzájemně autonomním prostředí z pohledu subjektu uživatele (administrátor organizace). Současně musí být podporována jednotná administrátorská správa (superadmin) z pohledu dodavatele služby – TCK KV a taktéž musí být zajištěna jednotná a jednoznačná technologie zálohování celého prostředí. |
| **Pořízení dat 1x, žádný dupl. vstup dat** | **N12** | Data pořizovaná v rámci ASW jsou vedena v ASW pouze jednou, není požadován duplicitní vstup dat. Je zajištěna jednoznačnost vstupních informací a jejich následné sdílení a provazování s jinými záznamy. |
| **Provoz v Rowanetu při výpadku Internetu** | **N23** | ASW musí být schopen autonomního provozu v regionální síti ROWANet i v případě omezené nebo zcela nedostupné konektivity do Internetu. |
| **2s pro zápis údaje v aplikaci (při rychlosti 0,5 Mb/s)** | **N24** | Z pohledu uživatele (UI) musí být schopen systém uložit jakýkoliv uživatelem zadaný popisný údaj (do max velikosti 1KB; nikoliv binární přílohu) do 2s i při rychlosti spojení klienta 0,5Mb/s |
| **Logování a historizace všech operací** | **N25** | ASW podporuje kompletní logování a historizace všech operací prováděných ze strany uživatelů, integrovaných systémů a interních procesů systémů s vlivem na datový obsah a bezpečnost. |
| **Podporuje autonomní databáze pro jednotlivé subjekty** | **N26** | ASW podporuje virtualizace na úrovni autonomních databází nikoli na bázi celých serverových instalací, aby bylo možno jednotně spravovat více autonomních instancí ASW pro více subjektů. |
| **Export DB a odchod organizace z hostingu do svého prostředí** | **N27** | ASW umožňuje export dat organizace do samostatné databáze a její případné provozování přímo v dané organizaci (odchod organizace z multitenantního krajského řešení a provozování ve vlastním) |
| **Integrace s jiný aplikacemi (přes API SOAP nebo REST)** | **N28** | Preferovaný způsob integrace s ostatními aplikacemi je využití technologie SOAP (web služby WS) nebo REST (HTTPS). Výměna dat pomocí těchto integračních vazeb nesmí proběhnout bez předchozí autentizace a autorizace. |
| **Výměna dat s jinými apl. (XML)** | **N29** | Výměnný formát podporovaný na úrovni API je strukturované a dokumentované XML nebo JSON |
| **Vzdálená aktualizace bez nutnosti jakýchliv inst. na koncových zař.** | **N30** | Aktualizace ASW probíhá ve formě vzdálené aktualizace celého řešení bez nutnosti instalace komponent na koncových stanicích a bez nutnosti instalace na místě (on-site) v datovém centru kromě předem definovaných specifických situací. |
| **Inst. balíček+DOK+inst. instrukce** | **N31** | Pokud je řešení dodáváno jako desktopová aplikace, je pro instalaci ASW požadováno dodání instalačního balíčku (package) včetně dokumentace a instalačních instrukcí |
| **Zálohování a arch. za provozu** | **N32** | Průběžné zálohování a archivaci ASW je možno provádět za provozu aplikace, není požadováno zastavení systému. |
| **Zálohování a arch. pracovníky z OI** | **N33** | Zálohování a archivaci dat ASW je možno provádět interně určenými pracovníky KV (typicky odbor IT) bez součinnosti dodavatele |
| **Licence pro dvě prostředí (PROD+TEST)** | **N34** | V rámci dodávky licencí je požadován dodání minimálně 2 prostředí (produkční a testovací), optimálně 3 prostředí (produkční, testovací a školící). |
| **Dokumentace v CZ (odborné věci možno v AJ)** | **N35** | Dokumentace k ASW je dodána v českém jazyce, přípustnou výjimkou je dokumentace ryze technického resp. systémového charakteru, kde je možné dodání dokumentace v jazyce anglickém. |
| **Kontext. nápověda v CZ** | **N36** | Součástí ASW je kontextová nápověda v českém jazyce |
| **Trvalé (perpetuální) licence** | **N37** | Licence ASW je trvalá, časově neomezená |

**Akceptační testy:**

* zaevidování alespoň 1 předmětu do každé podsbírky
* vytvoření nového tenantu (organizace)
* přihlášení uživatele prostřednictvím krajské identity
* přidělení a odebrání editační role uživateli pro danou podsbírku
* přenos dat do systému e-sbírky
* přenos dat do systému CES
* export dat za vybranou sbírku