Příloha K.1 Smlouvy

Kvalitativní vlastnosti Projektu a Služeb TIS

1. KONVENCE TOHOTO DOKUMENTU

1.1. Obecné

1.1.1. Pro potřeby Zadání jsou zkratkou TIS označeny všechny části informačního systému Teiresiás. Slovem web je pak označen výstup TIS v prohlížeči uživatele.

1.1.2. Slovem administrace jsou pak označeny všechny editační, administrační rozhraní a nástroje, které pro Zákazníka vytvořil nebo vytváří Dodavatel.

1.1.3. Všechny body požadavků jsou uvedeny v přítomném či minulém čase a pokud možno bez použití kondicionálů proto, aby každý požadavek šlo vyhodnotit jako splněný či nesplněný jednoduchou odpovědí ano / ne podle jeho aktuálního reálného stavu v době akceptace. Použití minulého času v tomto dokumentu neznamená automatické potvrzení Zákazníka o splnění tohoto bodu. Splnění či nesplnění požadavku je vždy předmětem akceptačního řízení.

1.1.4. Pokud z kontextu nevyplývá jinak, slova a slovní spojení v jednotném čísle zahrnují i množné číslo a naopak.

1.1.5. Zkratkou IS nebo IS MU se rozumí Informační Systém Masarykovy univerzity.

1.1.6. Zkratkou SLI (Service Level Indicator) se rozumí sledované metriky TIS nebo Služeb, které Zákazníkovi poskytuje Dodavatel.

1.1.7. Zkratkou SLO (Service Level Objective) se rozumí konkrétní hodnoty (cíle) nebo rozsahy hodnot jednotlivých SLI. Pro jedno SLI může být více SLO (nedodržení cíle může znamenat různý typ incidentu).

OBSAH DOKUMENTU

2. ORGANIZAČNÍ A PRÁVNÍ POŽADAVKY

2.1. Obecné

2.1.1. Dodavatel se zavazuje vytvořit TIS a každou jeho část tak, aby jejich další změny či rozvoj mohl po skončení Smlouvy realizovat kterýkoliv jiný odborník v oboru. To znamená, že Dodavatel:

a. bude psát veškeré zdrojové kódy, které budou předány Zákazníkovi, podle nejnovějších a nejlepších standardů, v přehledné a strukturované formě a bude je přehledně a srozumitelně komentovat;
b. ke všem funkcionalitám TIS bude vést písemnou Dokumentaci, kde budou popsány jednotlivé funkce, logické a technické vazby mezi nimi, vysvětlivky a další potřebné informace, aby mohl na rozvoj TIS či jeho změny navázat bez obtíží jiný odborník v oboru.
c. bude odborně, kapacitně i personálně připraven po skončení smlouvy poskytnout součinnost a za stejných cenových podmínek jako při poskytování servisních služeb předat Dílo další straně, kterou určí Zákazník.

2.2. Organizační požadavky

2.2.1. Všechny komplexní požadavky na systém vychází z provedených detailních analýz požadavků a jsou zpracovány v písemné podobě kterou schvaluje Zákazník.

2.2.2. Všechny externí služby, které má Dodavatel záměr použít, jsou písemně schváleny Zákazníkem. Účty k těmto službám jsou vytvořeny na správcovský účet ve vlastnictví Zákazníka a Dodavatel má k těmto službám (pokud je třeba) nasdílen přístup na svůj samostatný účet.

2.3. Licence

2.3.1. Licence je upravena ve Smlouvě. Zákazník ke všem Výstupům, u kterých je to možné vzhledem k jejich charakteru, obdrží zdrojové soubory včetně dokumentace a komentářů a v případě zdrojových kódů i jejich kompletní historii.

2.3.2. Počet administrátorů (editorů) ani jiných osob a uživatelů (studentů) není licenčně omezen ani samostatně zpoplatněn.

2.3.3. Veškeré použité součásti nejsou zatíženy licenčními ani jinými podobnými periodickými poplatky.

2.4. Právní a další předpisy

2.4.1. Dodavatel při vytváření systému a poskytování služeb dodržuje právní předpisy a interní předpisy Zákazníka. Zákazník upozorňuje zejména na:

a. Nařízení (EU) 2016/679 (GDPR). Dodavatel vzal na vědomí a respektuje, že TIS pracuje se zvláštní kategorií osobních údajů.

b. Směrnice (EU) 2002/58/ES (Nařízení o soukromí a elektronických komunikacích) a Nařízení, které ji nahrazuje (ePrivacy).

c. Zák. č. 480/2004, zákon o některých službách informační společnosti a o změně některých zákonů, zejména §7.

d. Zákon 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

e. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

3. TECHNICKÉ POŽADAVKY

3.1. Domény a DNS

3.1.1. Kanonické URL TIS je https://tis.teiresias.muni.cz/.

3.1.2. Všechny nové registrace a prodloužení domén jsou zpracovávány Zákazníkem a na jeho odpovědnost.

3.1.3. DNS je ve správě Zákazníka a všechny změny podléhají schválení Zákazníkem. Dodavatel nemá přístup k administraci autoritativních DNS serverů. Dodavatel musí přizpůsobit vlastnosti systému a nastavit procesy tak, aby toto nezpůsobovalo prodlevy, výpadky či organizační problémy.

3.2. E-mail

3.2.1. Všechny e-maily, které jsou posílány jménem (tj. z domén) Zákazníka, jsou zasílány přes Zákazníkem předem schválené SMTP servery či služby, pro které jsou korektně nastavené DNS (SPF, DKIM atp.) záznamy.

3.2.2. E-maily odesílané z TIS nejsou posílané jménem (tj. z domény) návštěvníka/uživatele/partnera, pokud není zajištěna doručitelnost (SPF, DKIM, DMARC) těchto e-mailů.

3.2.3. E-mail obsahuje jméno odesílatele a subject v souladu s aktuálními best practices - např. délka, (ne)použití emojis, interpunkce, verzálek.

3.2.4. U HTML e-mailů existuje i TXT verze.

3.2.5. U e-mailů se používá preheader (“Johnson Box”).

3.2.6. E-mail je korektně zobrazen minimálně 90 % příjemcům a v nejpoužívanějších mailových klientech (Gmail, Seznam, Yahoo, Outlook, Apple mail) E-maily nemusí odlišovat “dark-mode” režim pro zobrazení e-mailů.

3.3. Internacionalizace a lokalizace

3.3.1. Celé řešení je realizováno s použitím kódování znaků UTF-8.

3.3.2. TIS je implementován v české a anglické jazykové verzi.

3.3.3. Řešení umožňuje zadávání a zobrazování dat pro všechny evropské země a oficiální jazyky EU (abeceda, řazení, směr psaní, formáty čísel /např. telefon, PSČ, formátování čísel atp./, měna, fyzikální jednotky, formáty papíru, zvyklosti zápisu data a času včetně používání různých kalendářů a časových pásem).

3.3.4. Web je validní podle https://validator.w3.org/i18n-checker/.

3.3.5. Používá se HTML atribut lang.

3.4. Kompatibilita a interoperabilita

3.4.1. Jsou využity technologie standardizované organizacemi jako např. W3C, Ecma International, IEEE atp., které podporují přístupnost a kompatibilitu s různými výstupními zařízeními, tedy typicky validní HTML, CSS, JavaScript atd.

3.4.2. HTTP metody jsou používány korektně s ohledem na jejich idempotence / safety.

3.4.3. Dodavatel určil a zdokumentoval ve spolupráci se Zákazníkem relevantní šířky viewportu a pro tyto šířky je zobrazení webu testováno.

3.4.4. TIS plnohodnotně podporuje Referenční platformy, které jsou:

a. prohlížeče Google Chrome a Safari v posledních dvou hlavních verzích, nainstalované na počítači s operačním systémem macOS verze 10.15 a vyšší.

b. prohlížeče Microsoft Edge, Google Chrome a Mozilla Firefox v posledních dvou hlavních verzích, nainstalované na počítači s operačním systémem Microsoft Windows verze 10 a vyšší.

c. prohlížeč Safari, instalovaný na mobilním zařízení s operačním systémem Apple iOS v předposlední hlavní verzi a novější.

d. prohlížeč Google Chrome v posledních dvou hlavních verzích, instalovaný na mobilním zařízení s operačním systémem Android a Apple iOS.

3.4.5. Mimo referenční platformy se využívá přístupu pozvolné degradace (graceful degradation) pro zajištění co nejširší relevantní kompatibility.

3.5. Frontend / HTML, CSS, Obrázky, Video

3.5.1. Web má vhodné ikony a favicon pro všechny relevantní platformy.

3.5.2. Web neobsahuje odkazy vedoucí na neexistující adresy (HTTP 404).

3.5.3. Web nenačítá zdroje (CSS, JS, obrázky, ...) z neexistujících adres (HTTP 404).

3.5.4. Web má nastavený viewport stránky.

3.5.5. Používají se správné vstupní prvky (HTML5 input type) podle druhu zadávaných dat.

3.5.6. Používají se sémantické elementy HTML5 (header, section, footer, main ...).

3.5.7. Všechny hlavní šablony jsou testovány W3C validátorem pro identifikaci možných problémů.

3.5.8. V konzoli prohlížeče nejsou zalogovány žádné chyby ani ladící hlášení.

3.5.9. Při načítání webu nedochází k efektům FOIT (flash of invisible text).

3.5.10. Web používá responzivní design. Breakpointy jsou nastaveny podle analýzy zařízení návštěvníků. Web se přizpůsobuje vlastnostem a rozměrům výstupního zařízení z hlediska velikosti písma, rozměrů klikacích/dotykových prvků. U mobilních telefonů a tabletů proběhlo přizpůsobení dotykovému ovládání (minimální ergonomické rozměry dotykových prvků, nezávislost na hover stavech).

3.5.11. Všechna ID na stránce jsou unikátní.

3.5.12. Obrázky jsou poskytovány v alternativách dle podpory UA (nejlépe pomocí picture srcset, popř. dynamickou volbou mimetype dle UA). Alternativami jsou myšleny zejména relevantní případy vlastních obrázků:

a. vhodné rozměry obrázku podle výstupního zařízení (malé, velké)

b. vhodné formáty obrázku s přihlédnutím zejména na datovou velikost a charakter obrazové informace (preferovány moderní formáty SVG, WebP, JPEG 2000, JPEG XR, AVIF atp.).

3.5.13. Stránky, které dává na základě analýzy smysl tisknout, jsou upraveny pro tiskový výstup pomocí tiskových stylů. Tiskové výstupy jsou optimalizovány tak, aby spořily spotřební materiál uživatele (papír, toner).

3.6. Optimalizace pro vyhledávače

3.6.1. Není zakázaná indexace veřejného a publikovaného obsahu vyhledávači, pokud toto nevyplývá z explicitního funkčního požadavku.

3.6.2. Je nasazen korektní robots.txt.

3.6.3. Stejný obsah webů není duplicitně přístupný na více URL a na jednom URL není přístupno více stránek. Za různá URL se považují i URL lišící se jen počtem či hodnotami parametrů ("query").

3.6.4. URL webů nemá nadbytečné parametry nebo obsah v částech URL "query", či "path" a je co nejkratší (při zachování čitelnosti a dodržení SEO zadání či potřeb).

3.6.5. V částech "path" a "fragment" a názvech a hodnotách části "query" URL webů se používají jen písmena anglické abecedy, číslice, pomlčky (minus), tečky a lomítka.

3.7. Přístupnost

3.7.1. Jsou respektována Web Content Accessibility Guidelines 2.1 minimálně v úrovni shody AA.

3.7.2. Systém a jeho výstupy jsou přístupné pro uživatele s libovolným typem postižení (např. postižení zraku, sluchu, pohybu a motoriky, specifické poruchy učení, psychické a neurologické onemocnění).

3.7.3. Používá se značkování WAI-ARIA v souladu s https://www.w3.org/TR/wai-aria-practices/

3.8. Rychlost

3.8.1. Není použitý "viewstate" ani podobný mechanismus komplikující cachování a zpomalující interakce s TIS.

3.8.2. CSS a JavaScript soubory jsou minifikované.

3.8.3. Používá se brotli, popř. gzip komprese a současně ochrana proti BREACH zranitelnosti u přenosu osobních či citlivých dat.

3.8.4. Obrázky jsou optimalizované, včetně uživatelsky nahrávaných.

3.8.5. JavaScript se načítá v maximální možné míře pomocí async nebo defer či jinou metodou, která zajišťuje neblokující vykreslování stránky.

3.8.6. V relevantních případech (dlouhé výpisy) se používá lazy loading obrázků.

3.8.7. Používají se jen nejnutnější cookies, session cookie se vytváří až je reálně potřeba (pro umožnění lepšího cachování).

3.8.8. Používá se maximálně 10 cookies, každá o max. velikosti 4 kB.

3.8.9. Assety (statický obsah) mají velmi dlouhou dobu uchovávání v cache (max-age či expires). Invalidace se provádí změnou názvu assetu.

3.8.10. Je použit protokol HTTP/2 na přístup ke všem zdrojům; výjimkou jsou externí služby, kde to dodavatel není schopen ovlivnit.

3.9. Zabezpečení

3.9.1. TIS netrpí základními zranitelnostmi, zejména

- Aktuální OWASP Top 10
- Obcházení autorizace - např. přístup k datům jiných zákazníků/uživatelů nebo funkcím správce z běžného účtu
- Nezabezpečené session ID - např. token, který lze uhodnout; token uložený na nezabezpečeném místě atp.
- Injections - SQLi, NoSQLi, XXE, OS command injection, …
- Cross-site scripting (XSS) - např. volání nezabezpečených funkcí JavaScriptu, provádění nezabezpečených manipulací s DOM, výpis uživatelského vstupu do HTML bez escapování.
- Cross-site request forgery (CSRF) - např. zpracování požadavků s hlavičkou Origin z jiné domény.
- Použití frontend i backend knihoven se známými zranitelnostmi
- Další zranitelnosti, které je možno detekovat běžnými automatizovanými nástroji

3.9.2. Nejsou veřejně přístupné interní a vývojové soubory a adresáře jako např. .git repozitář, konfigurační soubory pro vývoj, sestavení nebo provoz, source maps atp.

3.9.3. Jako zdroj aktuálních best practices je považován https://cheatsheetseries.owasp.org

3.9.4. Neexistují společné přístupové účty, každý pracovník Dodavatele i Zákazníka má samostatný přístup vedený na jeho jméno.

3.9.5. Uživatelé administrací mají k dispozici možnost aktivovat MFA (multi factor authentication, vícefaktorové ověřování). Pro role určené Objednatelem je použití MFA povinné.

3.9.6. Přístup k citlivým datům (osobní a přístupové údaje) je omezen výhradně na pracovníky s oprávněnou potřebou.

3.9.7. Oprávněná potřeba přístupu k citlivým datům je pravidelně kontrolována. Nadbytečné účty či přístupová oprávnění pracovníků bez oprávněné potřeby jsou bez zbytečného prodlení rušeny.

3.9.8. Je zajištěno, že neprodukční prostředí neobsahují produkční citlivá data. Dodavatel nekopíruje či nepřesouvá citlivá data z produkčního prostředí Zákazníka, pokud to Zákazník výslovně neschválil.

3.9.9. V případech, kdy systém zajišťuje autentizaci uživatelů, tak práce s hesly respektuje:

a. minimální délka hesla je 12 znaků pro běžné a 17 znaků pro administrátorské účty

b. maximální délka hesla není omezena na méně než 64 znaků

c. nejsou omezeny povolené znaky, které lze použít

d. nepoužívají se tajné otázky jako jediný požadavek na obnovení hesla

e. při změně hesla se vyžaduje aktuální heslo a e-mailové ověření změny

f. nově vytvořená hesla jsou

- ověřována podle seznamů běžných hesel
- algoritmicky kontrolována, že neobsahují opakování typu aaaa nebo sekvence typu 1234
- algoritmicky kontrolána, že v heslu není část e-mailu nebo jména uživatele či brandu, používaných značek Zákazníka

g. nově vytvořená hesla jsou ověřována podle databází uniklých hesel

h. hesla jsou ukládána v hashovaném a salted formátu za použití paměťově nebo výpočetně náročné jednosměrné hashovací funkce dle aktuálního doporučení NÚKIB v oblasti kryptografických prostředků

i. při detekci útoků pomocí hrubé síly je vynuceno vhodné uzamčení / ochrana proti přístupu k účtu

3.9.10. Ve Version Control System (VCS) nejsou uloženy žádná privátní hesla, certifikáty, klíče, přístupové údaje atp. (secrets). Výjimku tvoří secrets, které jsou společně s ostatními konfiguračními parametry uloženy v samostatném repozitáři a šifrovány bezpečným způsobem.

3.9.11. Je nasazen soubor security.txt podle posledního Internet-Draft nebo RFC.

3.9.12. V případě, že použitá součást obsahuje bezpečnostní chybu střední a větší závažnosti relevantní k systému, je součást aktualizována nejpozději do 30 kalendářních dnů, pokud je splněno:

a. Chyba má přidělený CVE identifikátor a současně

b. Existuje opravná verze či workaround od Dodavatele či autora této součásti

c. Nedošlo k písemné dohodě o tom, že se chyba nebude řešit

3.9.13. V případě, že použitá součást dle předchozího bodu obsahuje bezpečnostní chybu, které bylo přiděleno CVSS 3.x skóre >= 7, musí být použitá součást aktualizována nejpozději

a. do tří dnů pro CVSS 3.x skóre >= 9,

b. do sedmi dnů pro CVSS 3.x skóre >= 8,

c. do deseti dnů pro CVSS 3x skóre >= 7.

Jako počátek lhůty je považováno datum zápisu bezpečnostní chyby do databáze NIST NVD (NVD Published Date). Po uplynutí lhůty se nutnost aktualizace považuje za incident kategorie 2.

3.9.14. Externí zdroje se nenačítají z protocol-relative URL.

3.9.15. Pro všechna HTTPS URL je posílána Strict Transport Security hlavička.

3.9.16. Všechny cookie mají nastavený příznak Secure.

3.9.17. Session cookie mají nastavené příznaky HttpOnly a SameSite.

3.9.18. Významné akce, zejména v administrací, obsahují CSRF tokeny.

3.9.19. Používají se bezpečnostní hlavičky X-Frame-Options, X-Content-Type-Options, Referrer-Policy a Permissions-Policy.

3.9.20. Je definována bezpečná Content Security Policy (CSP).

3.9.21. Stránky při přístupu přes protokol HTTP korektně (tj. se zachováním FQDN) přesměrovávají na stejné URL s protokolem HTTPS.

3.9.22. Obsah a funkce jsou dostupné pouze pomocí protokolu HTTPS, přístup pomocí HTTP protokolu je umožněn pouze pro přesměrování na zabezpečenou variantu příslušného zdroje.

3.9.23. Všechny zdroje vkládané z jiných serverů, včetně iframes, jsou vloženy výhradně za použití protokolu HTTPS.

3.9.24. Je použit serverový certifikát schválený Zákazníkem. Jeho nasazování je automatizováno a platnost automaticky monitorována. Není použit certifikát s platností delší než 12 měsíců, klíč certifikátu se rotuje minimálně jednou ročně.

3.9.25. Není použito Public Key Pinning.

3.9.26. V URL není nikdy osobní údaj.

3.9.27. Na stránkách obsahujících osobní údaje není použit JavaScript načítaný od třetích stran, pokud není explicitně schválen Zákazníkem.

3.9.28. Načítání assetů (javascript, CSS, fonty, obrázky atp.) ze serverů třetí strany musí být vždy schváleno Zákazníkem. V těchto případech je vždy použito SRI (Subresource Integrity), pokud to server třetí strany podporuje.

3.9.29. V systému jsou implementovány všechny relevantní funkcionality, které vyžaduje GDPR s ohledem na zpracovávané osobní údaje. Výjimku tvoří operace, které manuálně provede Dodavatel v rámci poskytování Podpory.

3.9.30. Inline JavaScript (script type="text/javascript") je povolen pouze s nonce atributem, který se mění pro každý Request. Inline application/json je povolený i bez nonce.

3.9.31. Je veden záznam o servisních zásazích na Infrastruktuře s přesnými záznamy času, pracovníka a provedené operace.

3.9.32. Systém obsahuje opatření pro skokový nárůst Návštěvníků webových stránek či hackerské útoky.

3.10. Zakázané technologie

3.10.1. Není používána klientská technologie Adobe Flash, Microsoft Silverlight, Oracle Java ani podobná, vyžadující binární pluginy v prohlížeči uživatele.

3.11. Chybové stavy, chybové stránky

3.11.1. Požadavek na neexistující obsah vrací stavový kód HTTP 404. Chyba backend serveru vrací stavový kód HTTP 50x, údržba stavový kód HTTP 503 a při aplikaci rate limitingu je klientovi vrácen stavový kód HTTP 429.

3.11.2. Existují lokalizované error pages (400, 401, 403, 404, 503 /maintenance/, ostatní 4xx, 5xx); všechny tyto stránky jsou “custom”, jejich obsah se liší od standardních výchozích stránek webserveru.

3.12. Nasazování nových verzi

3.12.1. Součástí procesu vývoje a deploymentu je verzování databázových schémat a nastavení pro migraci dat nebo zajištění stejného či lepšího efektu, který tento požadavek zajišťuje.

3.12.2. Existuje více prostředí (minimálně vývojové, qa a produkční). Vývojovým prostředím je myšleno typicky lokální vývojové prostředí jednotlivého vývojáře či vnitrofiremní vývojové prostředí dodavatele. QA (Quality Assurance) prostředí je zpřístupněno Zákazníkovi pro testování funkčnosti a jedná se o prostředí technologicky velmi blízké produkčnímu prostředí (s menšími nároky na výkon a distribuovanost aplikace, pokud toto není předmětem

testování). Produkčním prostředím je míněno prostředí veřejně přístupné návštěvníkům a administrátorům webů.

3.12.3. Jediné prostředí, které je veřejně přístupné, je produkční prostředí.

3.12.4. Celý proces nasazování je vytvořen tak, že nasazení nové verze netrvá déle než 15 minut. Výjimku tvoří situace, kdy je nutné provést rozsáhlou migraci databáze - tyto ale Dodavatel provádí především v rámci servisního okna. Bezvýpadkové nasazení je preferováno, ale není vyžadováno.

3.12.5. O všech provedených nasazeních včetně přesných časů je veden záznam v helpdesku nebo monitorovacím systému.

3.12.6. Postup nasazování na libovolné běhové prostředí je stejný pro všechna prostředí s výjimkou vývojového prostředí a je plně automatizován.

3.13. Praktiky a metodiky

3.13.1. Jsou vybrány a definovány vhodné standardy pro zajištění čistoty zdrojového kódu (coding standards). Popis standardů je součástí dokumentace zdrojového kódu.

3.13.2. Zdrojové kódy jsou verzovány pomocí DCVS/CVS nástroje a uloženy v repozitářích. Zákazník má stálý read-only přístup ke všem těmto repozitářům. Popis verzovacího workflow je součástí dokumentace.

3.13.3. Změny zdrojového kódu jsou do repozitářů promítány nejméně 1x týdně.

3.13.4. Funkce, které je možné a vhodné (nejen technicky, ale zejména z business logiky) realizovat asynchronně, jsou takto řešeny (např. rozesílání e-mailů).

3.13.5. Je použit přístup “Secure by design”. Jsou použity frameworky, šablonovací jazyky nebo knihovny, které systémově řeší nedostatky implementace escapováním výstupů a sanitizací vstupů (např. ORM pro pro přístup k databázi, UI frameworky pro vykreslování DOM).

3.13.6. Dodavatel postupuje tak, aby nevznikal zbytečný technologický dluh. Technologickým dluhem je myšlen zejména:

a. důsledek postupů, které v zájmu krátkodobého zvýšení produktivity způsobí vznik provizorních řešení, která přinesou zvýšené náklady na vznik finálního řešení nebo jeho další rozvoj a údržbu;

b. důsledek nečinnosti, kdy se zastaráváním použitého řešení zvyšuje nákladnost aktualizace či provozu systému nebo kdy zastaralé řešení bude obsahovat bezpečnostně zranitelné součásti.

3.13.7. V případech, kde se vyplatí vědomě technologický dluh vytvořit a kde k takovému postupu Zákazník vyjádří souhlas není nutné dodržovat předchozí bod. Dodavatel upozornil Zákazníka na všechny případy, kdy identifikoval, že se vyplatí vytvořit technologický dluh.

3.14. Automatizace

3.14.1. Vývojový proces zahrnuje nástroje a postupy, které zajistí automatizovanou kontrolu dodržování coding standards (linter), pre/post procesory a compilery CSS či JS, buildovací a balíčkovací nástroje.

3.14.2. Všechny konfigurační soubory specifické pro aplikaci (například nastavení webového serveru, nastavení dalších komponent jako třeba Redis, MongoDB, Varnish cache apod.) jsou ukládány a verzovány v Git repozitáři, ke kterému má Zákazník read-only přístup. Tyto soubory se automaticky používají pro konfiguraci serverových součástí; u serverových součástí, kde toto není možné nebo by bylo neadekvátně nákladné, je toto nahrazeno dokumentací k ručnímu nastavení dané součásti.

3.14.3. Spolehlivost aplikace je testována minimálně prostřednictvím:

a. jednotkových testů pro knihovny a modely,

b. automatizovaných integračních a API testů,

4. POŽADAVKY NA DOKUMENTACI

4.1. Obecné

4.1.1. Veškerá dokumentace je v češtině nebo angličtině.

4.1.2. Veškerá dokumentace je tvořena tak, aby podporovala potřeby Zákazníka pro bezpečnostní, technické a další audity a kontroly veřejnými i soukromými společnostmi a orgány.

4.1.3. Zákazník má k dispozici uspořádané a přehledné výstupy všech provedených analýz.

4.2. Návrhová a vývojářská dokumentace

4.2.1. Dodavatel předal Zákazníkovi vývojářskou dokumentaci v písemné podobě, obsahující minimálně:

a. Popis základní logiky/filozofie produktu.

b. Popis logické architektury systému, všech jeho komponent a jejich vazeb včetně diagramů.

c. Dokumentace návrhu databáze.

d. Popis klíčových aplikačních entit a jejich vztahů

e. Dokumentace všech implementovaných síťových API (typicky RPC, REST, JSON API, GraphQL, SOAP, apod.)

f. Definice coding standards.

g. Popis release procesu.

h. Popis verzovacího workflow.

i. Testovací scénáře.

4.2.2. Popis deployment procesu; slovně a pomocí diagramu, z něhož budou patrné jednotlivé stavy a operace během vývoje a nasazování aplikace.

4.3. Provozní dokumentace

4.3.1. Dodavatel předal Zákazníkovi dokumentaci v písemné podobě, obsahující minimálně:

a. Dokumentace kompletní infrastruktury a repository s šablonami pro automatické nastavení infrastruktury.

b. Detailní instalační manuál.

c. Popis případných změn v nastavení operačních systémů.

d. Popis konfigurace aplikačních a webových serverů a konfigurací databází.

e. Seznam externích služeb, závislostí a datových toků (např. Mailchimp, Sentry, DataDog, CRM, ERP apod.)

f. Dokumentace periodických procesů (typicky cron jobs).

g. Dokumentace k používaným automatizacím (hooks, makefiles, playbooks, ...)

h. Dokumentace typů zasílaných e-mailů a způsobu jejich posílání (SMTP servery či služby a jejich požadavky na DNS záznamy).

i. Seznam standardních provozních úkonů a pracovních postupů pro správu systému.

j. Dokumentace k integracím či importům dat z externích zdrojů - zejména IS MU.

k. Detailní popis řešení zálohování a obnovy, včetně kompletních postupů Disaster Recovery. Dodavatel vytvořil a dále udržuje stále aktuální dokumentaci jednoznačně upravující kroky vedoucí k zajištění plné obnovy systému po havárii mající globální dopad na chod systému s ohledem na minimalizaci škod. Dokumentace DRP (Disaster Recovery Plan) je zpracována do nejmenšího detailu, to znamená vytvoření detailního postupu obnovy každé komponenty včetně popisu všech kroků vedoucí k její obnově. Pravidla zálohování obsahují vždy alespoň:

- specifikaci zálohovaných komponent (co je nutné zálohovat?)

- způsob jejich zálohování včetně časové návaznosti jednotlivých komponent (jakým způsobem se záloha má realizovat?)

- periodu zálohování (kdy / jak často se má záloha provádět?)
- retenční pravidla pro dobu a počet verzí uchovávaných záloh (jak dlouho a kolik verzí záloh se má uchovávat?)

l. Seznam administrátorských a servisních účtů k použitým operačním systémům, aplikacím a databázím.

m. Popis nastavení monitoringu a dohledu včetně použitých alertů a jejich konfigurace,

n. V samostatném dokumentu jsou evidovány metriky SLI a způsob jejich měření.

4.4. Bezpečnostní dokumentace

4.4.1. Dodavatel předal Zákazníkovi bezpečnostní dokumentaci v písemné podobě, minimálně v rozsahu:

a. Politika práce s hesly, klíči a certifikáty a způsob a místa jejich ukládání.

b. Seznam osobních údajů, se kterými systém pracuje.

c. Diagram, kudy putují osobní údaje systémem a kde jsou uložena.

d. Seznam třetích stran, které mají přístup k osobním datům a (odkaz na) smlouvy s těmito stranami

e. Popis použitých kryptografických prostředků, protokolů a nástrojů zejména pro účely auditů.

f. Tabulka požadovaných síťových prostupů, ke každé povolené komunikaci obsahuje alespoň:

- Zdrojová adresa / Skupina adres
- Cílová adresa / Skupina adres
- Cílový komunikační port / Skupina komunikačních portů
- Poznámka (Stručný text důvodu komunikace)

g. Seznam všech použitých TLS certifikátů s dobou platnosti včetně popisu a podrobného postupu pro jejich obnovu.

4.5. Uživatelská a business dokumentace

4.5.1. Existuje uživatelská dokumentace - návod na zadávání a úpravu obsahu. Dokumentace předpokládá základní dovednosti ovládání PC a intranetových aplikací. Zaměřuje se zejména

na specifika TIS a jednotlivé operace a postupy v něm prováděné. V dokumentaci jsou zachyceny významné důsledky a návaznosti jednotlivých operací.

4.5.2. Uživatelská dokumentace je členěná podle uživatelských rolí v systému a dále obsahuje podrobnosti o technickém zázemí systému.

5. SLEDOVANÉ UKAZATELE

5.1. Obecné

5.1.1. V samostatném provozním dokumentu jsou definovány SLI (Service Level Indicators - vyhodnocované metriky) a k nim příslušné SLO (Service Level Objectives - cíle dosahovaných SLI, většinou jako minimální či maximální hodnota, popř. rozsah hodnot - typicky za udaný čas). U SLI, u kterých to dává smysl se určuje region, ze kterého je prováděn test, referenční prohlížeč či obdobné údaje.

5.1.2. Dodavatel zajišťuje měření a vyhodnocování jednotlivých SLI.

5.1.3. V dokumentu jsou definovány typy sledovaných stránek (např. homepage, landing page, hledání, ...) a konkrétní sledovaná URL pro související SLI.

5.1.4. Dokument SLI/SLO byl odsouhlasen před předáním do testovacího provozu.

5.1.5. SLO uvedené tučně jsou minimální hodnoty v okamžiku uzavírání Smluv, po dohodě může být upraveno v dokumentu SLI/SLO. Pokud jsou nové hodnoty mírnější či nahrazeny za jiné, je změna SLO písemně oddůvodněna.

5.2. Dostupnost

5.2.1. Dodavatel zajišťuje dodržení minimální dostupnosti TIS **99 % měsíčně mimo Sezónu** a **99.9 % měsíčně v Sezóně**. Dodavatel není odpovědný za nedostupnost způsobenou nefunkčností infrastruktury či prostředků, které zajišťuje Zákazník, pokud dodrží Reakční lhůty.

5.2.2. Dosažená Dostupnost v procentech se vypočítá za každý kalendářní měsíc tak, že celkový počet celých minut, po který byla služba dostupná nebo probíhala plánovaná údržba v servisním okně, se vydělí celkovým počtem minut v měsíci a vynásobí 100. Pokud je mezi samostatnými nedostupnostmi období kratší než 10 minut, považuje se toto celé období za nedostupnost.

5.3. Rychlost

5.3.1. Systém je realizován tak, že je připraven na současné používání **150 uchazeči / studenty a 30 zaměstnanci** (uživatelé v administračním rozhraní) bez zaznamenatelného poklesu rychlosti. Systém musí být funkční i při současném používání **500 uchazeči / studenty a 80 zaměstnanci**. V tomto případě je akceptovatelné **navýšení doby odezvy až na 300 %**, nicméně systém je stále použitelný.

5.3.2. TTFB (Time To First Byte) pro statické soubory nebo dokumenty v cache **(max. 150 ms)**

5.3.3. Počet (v procentech) HTTP požadavků na "dokumenty" generované backendem (tj. ne požadavky assety) podle TTFB (Time To First Byte)

a. < 500 ms **(min. 20 %)**

b. 500 - 1.000 ms **(max. 80 %)**

c. 1.000 - 2.000 ms **(max. 10 %)**

d. > 2.000 ms **(max. 2 %)**

5.4. Ostatní

5.4.1. Pro všechna veřejně dostupná URL:

a. Qualys SSL Labs Test Grade **(A)**

b. Securityheaders.com Grade **(B)**

c. Mozilla Observatory Grade **(C)**

5.4.2. Pro celý TIS:

a. RTO (recovery time objective) **(168 hodin)**

b. RPO (recovery point objective) **(24 hodin)**

c. Četnost HTTP chyb 50x **(max 0.02 % celý systém)**