Kvalitativní vlastnosti

Příloha č. 2 ke smlouvě o dílo a servisní smlouvě

1. KONVENCE DOKUMENTU

1.1. Obecné

1.1.1. Tento dokument používá, a platí pro něj konvence, jak jsou definovány v Příloze č. 1 Smlouvy o dílo - Technické a věcné specifikaci.

2. ORGANIZAČNÍ A PRÁVNÍ

2.1. Obecné

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

a. bude psát veškeré zdrojové kódy, které budou předány Objednateli, podle nejnovějších a nejlepších standardů, v přehledné a strukturované formě a bude je přehledně a srozumitelně komentovat;
b. ke všem funkcionalitám Díla bude vést písemnou dokumentaci, kde budou popsány jednotlivé funkce, logické a technické vazby mezi nimi, vysvětlivky a další potřebné informace, aby mohl na rozvoj Díla 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 Objednatel.

2.2. Licence

2.2.1. Licence je upravena ve smlouvě o Dílo. Objednatel obdrží s Dílem kompletní zdrojové kódy a neomezenou nevýhradní licenci k užívání a modifikaci Díla.

2.2.2. Počet administrátorů (editorů) ani jiných uživatelů není licenčně omezen ani samostatně zpoplatněn.

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

2.3. Právní předpisy

2.3.1. Portál není informačním systémem veřejné správy ve smyslu zák. č. 365/2000.

2.3.2. Zhotovitel při vytváření Díla a poskytování Služeb postupuje v souladu s právními předpisy, Objednatel zejména upozorňuje na:

a. Zákon č. 99/2019 Sb. o přístupnosti internetových stránek a mobilních aplikací

b. Nařízení (EU) 2016/679 (GDPR)

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

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

e. Zákon 181/2014 Sb. o kybernetické bezpečnosti a následné vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti a soulad s interními bezpečnostními instrukcemi a politikami Objednatele.

3. TECHNICKÉ

3.1. Obecné

3.1.1. Zhotovitel používá Objednatelem určenou kanonickou doménu Webového portálu, pravděpodobně se bude jednat o doménu III. řádu na doméně justice.cz.

3.1.2. Celý Webový portál je realizován s použitím kódování znaků UTF-8.

3.1.3. Všechny externí služby, které má Zhotovitel záměr použít (včetně služeb jako Google Analytics, Google Tag Manager, Google Search Console …), jsou písemně schváleny Objednatelem. Účty k těmto službám jsou vytvořeny na správcovský účet ve vlastnictví Objednatele a Zhotovitel má k těmto službám (pokud je třeba) nasdílen přístup na svůj samostatný účet.

3.1.4. Návštěvnost webu je měřena a analyzována pomocí Google Analytics. Nad rámec základních měřících kódů jsou měřeny i relevantní uživatelské interakce (události) negenerující zobrazení nové stránky (URL) – např. spuštění YouTube videa. Případné pokročilé měření (např. Measurement Protocol) je součástí funkčních požadavků.

3.2. Domény a DNS

3.2.1. Všechny nové registrace a prodloužení domén jsou zpracovávány Objednatelem a na jeho odpovědnost.

3.2.2. DNS je ve správě Objednatele a všechny změny podléhají schválení Objednatelem. Zhotovitel musí přizpůsobit vlastnosti Webového portálu a nastavit procesy tak, aby toto nezpůsobovalo prodlevy, výpadky či organizační problémy.

3.3. E-mail

3.3.1. Všechny e-maily odesílané z Webového portálu (např. kontaktní formulář) jsou odeslané jménem Objednatele, tedy odesílatel je z domény Objednatele.

3.3.2. E-maily jsou zasílány přes Objednatelem předem schválené SMTP servery či služby, pro které jsou korektně nastavené DNS (SPF, DKIM atp.) záznamy.

3.3.3. Odesílaný e-mail obsahuje jméno odesílatele a subject v souladu s aktuálními best practices - např. délka, interpunkce, použití verzálek atp.

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

3.3.5. E-mail je korektně zobrazen minimálně 90 % příjemcům a v nejpoužívanějších mailových klientech (Gmail, Seznam, Yahoo, Outlook, Apple mail).

3.4. Internacionalizace a lokalizace

3.4.1. Webový portál je implementován v české jazykové verzi s jednostránkovou informací v angličtině. Některý obsah (zejména judikáty) jsou v anglickém či francouzském jazyce a funkce, které s takovým obsahem pracují (viz funkční zadání) s tímto počítají.

3.4.2. Webový portál umožňuje zobrazení a práci s daty pro všechny 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).

3.4.3. Weby jsou validní podle https://validator.w3.org/i18n-checker/.

3.5. Frontend (HTML, CSS, JavaScript)

3.5.1. Webový portál používá responzivní design. Webový portál 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).

3.5.2. Weby mají nastavený viewport stránky.

3.5.3. Všechna ID na stránce jsou unikátní.

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

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

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

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

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

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

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

3.6. Fonty

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

3.7. Obrázky a video

3.7.1. Videa jsou zajištěna skrze globální CDN řešení (přípustné i YouTube či Vimeo).

3.7.2. Obrázky se poskytují 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 X, AVIF atp.).

3.8. Přístupnost

3.8.1. 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).

3.8.2. U webů jsou respektována Web Content Accessibility Guidelines 2.1 minimálně v úrovni shody AA.

3.8.3. U webů se používá značkování WAI-ARIA v souladu s https://www.w3.org/TR/wai-aria-practices/

3.8.4. Web 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).

3.9. Rychlost

3.9.1. Není použitý "viewstate" ani podobný mechanismus komplikující cachování a zpomalující interakce s webem.

3.9.2. HTML, CSS a JavaScript soubory jsou minifikované.

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

3.9.4. Obrázky jsou optimalizované, včetně uživatelsky nahrávaných.

3.9.5. JavaScript se načítá v maximální možné míře pomocí async nebo defer.

3.9.6. V relevantních případech (dlouhé výpisy) se používá lazyloading obrázků.

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

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

3.9.9. Používá se dns-prefetch.

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

3.10. Technické SEO

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

3.10.2. Na weby je nasazen korektní robots.txt.

3.10.3. Pro weby existuje relevantní, validní a aktuální Sitemap v XML formátu podle https://www.sitemaps.org/. V případě většího rozsahu (limit 50.000 záznamů nebo 50MB nekomprimovaně) je Sitemap rozdělena do více souborů uvedených v Sitemap index souboru. Může být použita gzip komprese. Sitemap je korektně odkázána v robots.txt.

3.10.4. Webový portál robotům neblokuje přístup ani neposkytuje rozdílný obsah. Případné blokování zajišťuje Objednatel a probíhá na úrovni jeho infrastruktury dle aktuálních nastavení a bezpečnostních politik.

3.10.5. Stejný obsah webového portálu není duplicitně přístupný na více URL a na jednom URL není přístupné více stránek. Za různá URL se považují i URL lišící se jen počtem či hodnotami parametrů (“query”).

3.10.6. URL stránek není zbytečně dlouhé a obsahuje pouze parametry, cesty či jiné řetězce, které jsou nezbytné pro funkci nebo vhodné z jiných důvodů (SEO, informační architektura atp.).

3.10.7. V URL stránek se používají jen malá písmena anglické abecedy, číslice, pomlčky (minus), tečky a lomítka.

3.10.8. Title a description stránek webu jsou automaticky generována z nadpisů či obsahu stránky, každá stránka má unikátní title. Je možné definovat vlastní title a description.

3.10.9. Na každé veřejné stránce jsou implementovány náhledy pro sociální sítě. Open Graph a Twitter Cards minimálně v rozsahu reprezentativního obrázku.

3.10.10. Nad rámec základního HTML obsahuje zdrojový kód stránek i validní sémantické značkování vybraných objektů (události, místa, osoby apod.) podle specifikace Schema.org JSON-LD.

3.10.11. Hlavní obsah, položky navigace webu a hledání jsou dostupné bez JavaScriptu.

3.11. Kompatibilita a interoperabilita

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

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

3.11.3. Webový portál se zobrazuje korektně i se zapnutými nejběžnějšími adblockery.

3.11.4. Webový portál je testován minimálně pro tyto šířky viewportu (Bootstrap 5 breakpoint ekvivalent):

a. Mobile portrait (xs) 375 px

b. Mobile landscape, tablet portrait (lg) 768 px

c. Tablet landscape, desktop (xl) 1280 px

d. Desktop (xxl) 1920 px

3.11.5. Webový portál 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.

3.12. HTTPS

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

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

3.13. Zakázané technologie

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

3.14. Chybové stránky

3.14.1. 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.

3.14.2. 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.

3.15. Zabezpečení

3.15.1. Webový portál netrpí základními zranitelnostmi podle OWASP Top 10 (např. XXE, XSS, SQLi), které je možno detekovat běžnými automatizovanými nástroji. Nejsou veřejně přístupné interní a vývojové soubory a adresáře jako např. .git repozitář, konfigurační soubory pro vývoj, sestavení nebo provoz atp.

3.15.2. Jako zdroj aktuálních best practices je považován https://cheatsheetseries.owasp.org, zejména při práci s přihlašovacími a osobními údaji uživatelů.

3.15.3. Neexistují společné přístupové účty, každý pracovník Zhotovitele má samostatný přístup vedený na jeho jméno.

3.15.4. Práce s hesly (požadavky na složitost, autentizace) respektuje minimálně požadavky NIST Special Publication 800-63B 5.1.1.2 specifikované slovy SHALL, SHOULD, SHOULD NOT.

3.15.5. V systému správy verzí zdrojového kódu (VCS) nejsou uloženy žádná funkční hesla, klíče ani přístupové údaje.

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

3.15.7. V případě, že použitá součást obsahuje bezpečnostní chybu, 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 Zhotovitele či autora této součásti

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

3.15.9. Všechny HTTPS URL obsahují Strict Transport Security hlavičku.

3.15.10. Všechny cookie mají nastavený příznak Secure.

3.15.11. Session cookie mají nastavené příznaky HttpOnly a SameSite.

3.15.12. Významné akce obsahují CSRF tokeny.

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

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

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

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

3.15.17. Není použito Public Key Pinning.

3.15.18. V URL není nikdy osobní údaj.

3.15.19. Na stránkách obsahujících osobní údaje je minimalizováno použití JavaScriptu načítaného od třetích stran. V těchto případech je vždy použito SRI (Subresource Integrity) pokud je podporované vendorem příslušného JS nebo se Zhotovitel dohodl se Objednatelem na výjimce.

3.15.20. Ve Webovém portálu jsou implementovány všechny relevantní funkcionality, které vyžaduje GDPR s ohledem na zpracovávané osobní údaje. Výjimku tvoří operace, které manuálně provede Zhotovitel v rámci poskytování Podpory.

3.16. Verzování zdrojového kódu

3.16.1. Zdrojové kódy jsou kontinuálně a od začátku vývoje verzovány pomocí Git (https://git-scm.com). Popis verzovacího workflow je součástí dokumentace.

3.16.2. Je využíván GitLab server Objednatele pro verzování i nasazování nových verzí.

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

3.17. Coding standards

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

3.18. Automatizace

3.18.1. 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.

3.18.2. Všechny konfigurační soubory specifické pro aplikaci (například nastavení webového serveru, nastavení dalších komponent jako třeba Redis, MongoDB apod.) jsou ukládány a verzovány v Git repozitáři na Git serveru Objednatele. 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.

3.19. Nasazování nových verzí

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

3.19.2. Existuje více prostředí (minimálně vývojové, Testovací a Produkční). Vývojovým prostředím je myšleno typicky lokální vývojové prostředí jednotlivého vývojáře či vnitrofiremní vývojové prostředí Zhotovitele. Na Testovacím prostředí provádí Objednatel testování funkčnosti a jedná se o prostředí technologicky velmi blízké Produkčnímu prostředí (s menšími nároky na výkon aplikace, pokud toto není předmětem testování). Produkčním prostředím je míněno prostředí veřejně přístupné návštěvníkům a administrátorům webů. Provoz vývojového prostředí zajišťuje Zhotovitel, ostatní prostředí zajišťuje Objednatel.

3.19.3. Pro vývoj a deployment jsou použity techniky a nástroje, které umožní minimálně částečné automatizované nasazování a testování nových verzí aplikace. Popis nasazování je součástí dokumentace. Součástí deploymentu je automatizace přinejmenším těchto operací nebo zajištění stejného či lepšího efektu, který tyto operace poskytují:

a. build aplikace (včetně generování CSS a JS skriptů apod.),

b. přenos na cílové prostředí a kontrola závislostí,

c. přepnutí aplikace do maintenance modu (pokud je nutné),

d. migrace DB pomocí rozdílových skriptů,

e. výměna aplikačního kódu,

f. vypnutí maintenance modu (pokud je nutné).

3.19.4. Postup nasazování na prostředí, které zajišťuje Objednatel, je stejný pro všechna prostředí.

3.20. Praktiky

3.20.1. Funkce, které je vhodné (technicky i z business logiky) realizovat asynchronně, jsou takto řešeny.

3.20.2. Je použit přístup “Secure by design”.

3.20.3. Web je připraven pro load balancing a použití více než jednoho aplikačního backendu.

3.20.4. Web je vhodně navržen pro použití víceúrovňového cachování (SQL dotaz, funkce, fragment, stránka) a je možné ji umístit a provozovat za proxy cache / HTTP akcelerátor (např. Varnish).

4. DOKUMENTACE

4.1. Obecné

4.1.1. Veškerá uživatelská či business dokumentace je v češtině. Technická dokumentace v češtině nebo angličtině.

4.1.2. Veškerá dokumentace je tvořena tak, aby podporovala potřeby Objednatele zejména z pohledu zajištění provozní infrastruktury a pro bezpečnostní, jiné technické a další audity. Rozsah a forma dokumentace může být doplněna dohodou Zhotovitele a Objednatele ve Fázi 1.

4.1.3. Objednatel obdrží uspořádané a přehledné výstupy všech provedených analýz.

4.2. Návrhová a vývojářská dokumentace

4.2.1. Zhotovitel předá Objednateli vývojářskou dokumentaci v písemné podobě, obsahující minimálně:

a. Popis základní logiky/filosofie produktu.

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

c. Dokumentace návrhu databáze.

d. Popis klíčových aplikačních entit a vztahů.

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

f. Detailní dokumentace integrace na datové zdroje právních rozsudků.

g. Definice coding standards.

h. Popis release procesu.

i. Popis verzovacího workflow.

j. Testovací scénáře.

4.3. Provozní dokumentace

4.3.1. Zhotovitel předá Objednateli provozní dokumentaci v písemné podobě, obsahující minimálně:

a. Dokumentace kompletní infrastruktury.

b. Detailní instalační manuál.

c. Popis případných změn v nastavení operačních systémů

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

e. Doporučení nastavení loadbalanceru (viz provoz) včetně healthchecks, affinity a session persistence v případě, že bude loadbalancer pro Webový portál použit.

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

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

h. Dokumentace periodických procesů (typicky cron jobs).

i. Dokumentace k používaným automatizacím (hooks, makefiles, playbooks, …).

j. Dokumentace k integracím či importům dat z externích zdrojů.

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

l. Seznam standardních provozních úkonů a pracovních postupů pro správu Webového portálu.

m. Detailní popis řešení zálohování a obnovy, včetně kompletních postupů Disaster Recovery. Zhotovitel ve fázi 6 vytvořil a dále udržuje stále aktuální dokumentaci jednoznačně upravující kroky vedoucí k zajištění plné obnovy Webového portálu po havárii mající globální dopad na chod Webového portálu s ohledem na minimalizaci dopadů. 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. Plány obnovy musí být také v souladu s poskytnutou metodikou plánů obnovy Objednatele. Objednatel předpokládá, že bude zajišťovat obnovu Webového portálu do úrovně běžícího operačního systému. Zhotovitel pak odpovídá za obnovu aplikací, databází a úložiště dokumentů. 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?)

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

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

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

4.4. Bezpečnostní dokumentace

4.4.1. Zhotovitel předá Objednateli bezpečnostní dokumentaci v písemné podobě, minimálně v rozsahu:

a. Dokumentace k zabezpečení (VPN, ukládání hesel, TLS atp) zejména pro účely auditů.

b. 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)

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

d. Popis použitých kryptografických prostředků.

4.5. Uživatelská a business dokumentace

4.5.1. Zhotovitel předá Objednateli uživatelskou dokumentaci v písemné podobě, obsahující minimálně:

a. Návod na zadávání a úpravu obsahu. Může odkazovat na dokumentaci použitého CMS. Může mít formu webové stránky dostupné přímo z rozhraní aplikace.

b. Dokumentace pro uživatele veřejné části Webového portálu. Může mít formu webové stránky dostupné přímo z rozhraní aplikace.

c. Dokumentace pro administrátorské role aplikace, včetně popisu správy uživatelů, rolí a jejich oprávnění.

5. SLEDOVANÉ UKAZATELE

5.1. Obecné

5.1.1. V samostatném provozním dokumentu budou 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 testování rychlosti pomocí webpagetest.org zahrnuje SLO region, z jakého je prováděn test.

5.1.2. Zhotovitel 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 zahájením fáze 6 - Předání do pilotního 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, je změna SLO písemně oddůvodněna.

5.2. Dostupnost

5.2.1. Zhotovitel zajišťuje dodržení **minimální dostupnosti webů 99 % a administrace 95 %** měsíčně. Zhotovitel není odpovědný za nedostupnost způsobenou nefunkčností infrastruktury či prostředků, které zajišťuje Objednatel, 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. Zátěž

5.3.1. Webový portál je realizován tak, že je připraven na současné používání **250 návštěvníků a 5 administrátorů** bez zaznamenatelného poklesu rychlosti. Webový portál musí být funkční i při současném používání **500 návštěvníky a 10 administrátory**. V tomto případě je akceptovatelné **navýšení rychlosti odezvy až na 300 %**, nicméně web i administrace jsou stále použitelné pro práci.

5.4. Rychlost

5.4.1. Jako referenční prostředí pro desktopové měření rychlosti se považuje:

a. Prohlížeč Google Chrome v poslední stabilní verzi
b. Velikost displeje 1920x1280 (1080p, Full HD)
c. Konektivita Cable (5/1 Mbps 28ms RTT)

5.4.2. Pro všechna veřejná URL získávaná GET metodou

a. Core Web Vitals (LCP, FID, CLS) - (good - “all green”)
b. Google PageSpeed Insights Score Mobile / Desktop **(80/80)**
c. TTFB (Time To First Byte) **(max. 350 ms)**

5.5. Ostatní

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

b. Securityheaders.com Grade **(C)**
c. Mozilla Observatory Grade **(D)**
d. RTO (recovery time objective) **(168 hodin)**
e. RPO (recovery point objective) **(24 hodin)**
f. Četnost HTTP chyb 50x **(max 0.02 % celý Webový portál)**