SMLOUVA O DÍLO

uzavřená podle § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“)

Kraj Vysočina
se sídlem: Žižkova 1882/57, Jihlava
IČO: 70890749
Zastoupený: Mgr. Vítězslavem Schrekem, hejtmanem kraje
K podpisu smlouvy pověřen: RNDr. Jan Bříždala, radní kraje
(dále jen „**Objednatel**“)

a

WEBHOUSE, s.r.o.
se sídlem/místem podnikání: Levského 3187/6 14000 Praha 4/Brněnská 602/26 58601 Jihlava
IČO: 25327054
DIČ: CZ25327054
zapsaná v obchodním rejstříku pod sp. zn. odd. C, vl. 593 57 vedenou u městského soudu v Praze
bankovní spojení: KB Jihlava, UniCredit Bank Jihlava
číslo účtu: 19-4661040227/0100, 2111447517/2700
za kterou jedná: Ing. Jitka Savická
(dále jen „**Zhotovitel**“)

uzavřeli níže uvedeného dne, měsíce a roku

tuto smlouvu:

Čl. I
Předmět smlouvy

1. Objednatel a Zhotovitel uzavírají tuto smlouvu o dílo v rámci zakázky s názvem Nové webové stránky Kraje Vysočina (dále jen „veřejná zakázka“).
2. Předmětem této smlouvy je závazek Zhotovitele v rozsahu a za podmínek stanovených touto smlouvou pro Objednatele provést dílo, které je předmětem veřejné zakázky, jak je blíže specifikováno v této smlouvě a její příloze č. 1 a č. 2 a tak, aby dílo bylo provedeno jako úplné a byl naplněn účel jeho provedení (dále jen „dílo“).

   Závazkem Objednatele je řádně a včas dokončené dílo převzít a zaplatit za něj Zhotoviteli cenu díla stanovenou v čl. IV této smlouvy a za podmínek uvedených v této smlouvě.
3. Zhotovitel bere na vědomí, že:
   - Objednatel je povinnou osobou dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti,
   - Dílo je dle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích kategorizováno jako významný informační sytém dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících právních předpisů a že
   - Zhotovitel se stává významným dodavatelem Objednatele.

Čl. II
Provádění díla

1. Smluvní strany se dohodly, že dílo je provedeno poskytnutím dodávek a prací uvedených v zadávací dokumentaci veřejné zakázky, její příloze č. 1, nabídce Zhotovitele zpracované a podané v souladu se zadávacími podmínkami veřejné zakázky, a za podmínek uvedených v této smlouvě.
2. Zhotovitel je povinen provést veškeré dodávky, činnosti, služby a výkony, kterých je potřeba k zahájení, dokončení a předání díla, ve vysoké kvalitě s náležitou a odbornou péčí, a obstarat vše, co je k provedení díla potřeba. Dílo bude provedeno tak, aby jeho řádnému užití nebránila práva třetích osob.
3. V rámci provádění díla musí Zhotovitel přebrat veškeré závazky vyplývající z jeho činnosti ve smyslu zákona o životním prostředí a nakládání s odpady. Při provádění díla je Zhotovitel současně povinen dodržovat předpisy na úseku ochrany životního prostředí, odpadového a vodního hospodářství a zejména na vlastní účet a v souladu s platnými právními předpisy provádět odvoz a řádnou likvidaci odpadů. Náklady na veškeré tyto činnosti jsou zahrnuty v ceně díla.
4. Smluvní strany se zavazují informovat se navzájem o všech skutečnostech, které mají, nebo by mohly mít, vliv na plnění této smlouvy.
5. Smluvní strany jsou povinny poskytovat si nezbytnou součinnost k plnění této smlouvy.
6. Objednatel je oprávněn poskytovat Zhotoviteli v průběhu provádění díla pokyny k jeho provádění a kontrolovat provádění díla.
7. Zhotovitel postupuje při provádění díla samostatně, je však povinen dbát pokynů Objednatele a pokynů oprávněné a kontaktní osoby Objednatele dle této smlouvy.
8. Zhotovitel je povinen upozornit Objednatele na zřejmě nesprávný pokyn, a to bez zbytečného odkladu, a s jeho plněním vyčkat až do doby, než Objednatel písemně potvrdí Zhotoviteli, že na splnění pokynu i přesto trvá.
9. Ustanovení odst. 5 nevylučuje právo Objednatele požadovat nedodání některé položky předmětu díla či její poměrné části dle přílohy č. 1 této smlouvy v případě, že zjistí, že z technických, finančních či organizačních důvodů není jejich dodání či poskytnutí možné nebo vhodné. Pokyn Zhotoviteli k neprovedení plnění je v takovém případě oprávněna vydat kontaktní osoba Objednatele dle čl. VI odst. 2.
10. Plnění nad shora sjednaný obsah a rozsah díla (vícepráce) bude realizováno, jen pokud o ně bude dílo rozšířeno po vzájemné dohodě písemným dodatkem k této smlouvě.
11. Při realizaci díla je Zhotovitel povinen dodržovat veškeré vnitřní předpisy Objednatele vztahující se k takovým činnostem, které Objednatel Zhotoviteli již poskytl ke dni uzavření této smlouvy, popř. dále poskytne před zahájením takových činností.
12. Zhotovitel není oprávněn postoupit práva, povinnosti, závazky a pohledávky z této smlouvy třetím osobám bez předchozího písemného souhlasu Objednatele.
13. Výsledky vznikající v rámci činností Zhotovitele při provádění díla Zhotovitel není oprávněn poskytnout jiným osobám, než jak je založeno touto smlouvou, bez předchozího písemného souhlasu Objednatele.
14. Zhotovitel odpovídá v plném rozsahu za dodávky, práce a činnosti prováděné jeho zaměstnanci a poddodavateli, seznámí je vždy se všemi dohodnutými podmínkami provádění prací, jakož i smluvními termíny sjednanými v této smlouvě.
15. Nedostatky a vady díla zjevné již v průběhu dodání, montáže či instalace, či poskytovaných souvisejících služeb je Zhotovitel povinen na vyzvání Objednatele bez zbytečného odkladu odstranit.
16. Objednatel má právo dle svého uvážení užívat všechny výstupy vzniklé v rámci provádění díla a poskytovat je dle svého uvážení dalším osobám.
17. Zhotovitel je povinen zajistit bezpečnost informací a mlčenlivost v souvislosti s prováděním díla dle čl. XI této smlouvy.

Čl. III
Doba a místo plnění

1. Zhotovitel je povinen dílo provést a jednotlivé jeho části, výstupy a výsledky činností Zhotovitele uvedené v této smlouvě a její příloze č. 1 a předat je Objednateli v termínu do do 31. 12. 2023 v souladu s harmonogramem dle přílohy č. 1.
2. Zhotovitel je povinen bezodkladně písemně informovat Objednatele o veškerých okolnostech, které mohou mít vliv na termín dokončení provedení díla.
3. Místem plnění díla je sídlo zadavatele.
4. Zhotovitel je povinen při provádění díla dodržovat „Požadavky na bezpečnost webového portálu Kraje Vysočina“ uvedené v příloze č. 2 této smlouvy.

Čl. IV
Cena díla

1. Cena díla byla stanovena dohodou smluvních stran dle nabídky Zhotovitele ve výběrovém řízení a činí nejvýše 900 000 Kč bez DPH, tj. 1 089 000 Kč včetně DPH (slovy jedenmilionosmdesátdevěttisíc korun českých) splatná v etapách a částkách dle přílohy č.1.
2. Cena díla zahrnuje veškeré náklady na provedení díla v době a místě jeho plnění a za podmínek dle této smlouvy, zejm. veškeré dodávky, práce, výkony a služby, veškeré poplatky, dopravné, kterých je třeba pro včasné a kompletní provedení díla dle této smlouvy a veškeré další s tím související náklady Zhotovitele.
3. Cena díla je stanovena jako nejvýše přípustná a je možno ji změnit pouze za podmínek stanovených v této smlouvě, nebo zadávací dokumentaci veřejné zakázky.
4. Úprava ceny díla je možná v souvislosti se změnou daňových předpisů upravujících výši DPH, přičemž v takovém případě bude k dosud nesplacené části ceny díla připočtena DPH ve výši stanovené právními předpisy platnými a účinnými v době její úhrady.
5. Úprava sjednané ceny díla v průběhu jeho provádění včetně stanovení nové konečné ceny díla bude stanovena dohodou smluvních stran, a to formou písemného dodatku k této smlouvě.
6. Jakékoliv použití náhradních materiálů, jiných technologií či jiné odlišnosti plnění oproti příloze č. 1 této smlouvy je Zhotovitel povinen předem projednat a odsouhlasit s Objednatelem. Pokud Zhotovitel provede plnění nesjednané touto smlouvou bez předchozího projednání a odsouhlasení Objednatelem, není Objednatel povinen takové provedené plnění uhradit a může po Zhotoviteli požadovat bezplatné odstranění takového neodsouhlaseného plnění z místa plnění a/nebo obnovení původního stavu.

Čl. V
Platební podmínky

1. Objednatel neplatí Zhotoviteli žádnou zálohu v souvislosti s prováděním díla.
2. Cena díla bude uhrazena na základě faktury – daňového dokladu vystaveného Zhotovitelem po předání a převzetí díla. Faktura předložená Zhotovitelem Objednateli bude mít splatnost 30 dnů ode dne jejího prokazatelného doručení Objednateli.
3. Fakturu, která neobsahuje uvedené náležitosti, nebo jsou-li uvedeny nesprávně či neúplně, je Objednatel oprávněn vrátit Zhotoviteli. Při nezaplacení takto vystavené a doručené faktury není Objednatel v prodlení se zaplacením. Po doručení řádně vystavené faktury běží znovu sjednaná lhůta splatnosti.
4. Úhrada za plnění z této smlouvy bude realizována bezhotovostním převodem na účet Zhotovitele, který je správcem daně (finančním úřadem) zveřejněn způsobem umožňujícím dálkový přístup ve smyslu ustanovení § 98 zákona o DPH.
5. Pokud se po dobu účinnosti této smlouvy Zhotovitel stane nespolehlivým plátcem ve smyslu ustanovení § 106a zákona o DPH, smluvní strany se dohodly, že Objednatel uhradí

DPH za zdanitelné plnění přímo příslušnému správci daně. Objednatelem takto provedená úhrada je považována za uhrazení příslušné části smluvní ceny rovnající se výši DPH fakturované Zhotovitelem.

6. V souladu s ustanovením § 5 zákona č. 235/2004 Sb., o dani z přidané hodnoty, není Objednatel při přijímání výše uvedených zdanitelných plnění považován za osobu povinnou k dani, a proto tato zdanitelná plnění nebudou uskutečněna v režimu přenesení daňové povinnosti dle § 92a zákona o dani z přidané hodnoty. Daň z přidané hodnoty je tudíž povinen přiznat a zaplatit správci daně Zhotovitel jako plátce, který uskutečňuje zdanitelné plnění poskytnutí služby s místem plnění v tuzemsku.
7. Zhotovitel nemá právo požadovat během provádění díla přiměřenou část náhrady nákladů s přihlédnutím k vynaloženým nákladům jinak než, jak je uvedeno v této smlouvě.

Čl. VI
Kontaktní osoby

1. Kontaktní osobou Zhotovitele je: Vít Savický e-mail: vit.savicky@webhouse.cz, tel.: 736 777 625
2. Kontaktní osobou Objednatele je:
    a. Ve věcech smluvních: Petr Pavlinec, pavlinec.p@kr-vysocina.cz
    b. Ve věcech technických: František Bobek, bobek.f@kr-vysocina.cz

Čl. VII
Kontrola provádění díla

Objednatel je oprávněn kdykoliv během provádění díla provádět jeho kontrolu, a to buď sám, nebo prostřednictvím jiné osoby, a v případě, že zjistí nedostatky závažné plnění, zejména ohrožující život, majetek nebo zdraví či úspěšnou realizaci celého projektu, stanoví Zhotoviteli termín k bezodkladné nápravě. Pokud Zhotovitel v takto stanoveném termínu vytknuté nedostatky neodstraní, je Objednatel oprávněn od této smlouvy odstoupit.

Čl. VIII
Předání díla, jeho akceptace, vlastnické právo a nebezpečí škody

1. Zhotovitel se zavazuje předat Objednateli řádně provedené dílo.
2. Za řádně provedené dílo se považuje dílo dokončené, tj. způsobilé sloužit Objednateli k účelu vyplývajícímu z této smlouvy, popř. k účelu, který je pro užívání díla obvyklý, které Zhotovitel předá Objednateli v dohodnutém čase, na dohodnutém místě a bez vad.
3. Objednatel není povinen převzít předmět díla vykazující vady, má však právo převzít předmět díla vykazující drobné vady nebránící řádnému užívání předmětu díla a požadovat jejich odstranění v dohodnutém termínu.
4. Součástí předání díla je:
    - kontrola funkčnosti díla s možností ovládání jeho uživateli,
    - zaškolení oprávněných osob Objednatele v rozsahu nezbytném pro řádné užívání díla.
5. Zhotovitel písemně oznámí Objednateli nejpozději 5 dnů předem, kdy bude dokončené dílo připraveno k předání a převzetí.
6. Po řádném předání a převzetí díla Zhotovitel předloží Objednateli předávací protokol, na kterém oprávněný pracovník Objednatele potvrdí řádné převzetí dokončeného díla. Oprávněným pracovníkem Objednatele je František Bobek, email: bobek.f@kr-vysocina.cz, tel.: 724 650 232. Každá smluvní strana obdrží jedno vyhotovení oboustranně potvrzeného předávacího protokolu, který se tak stane dokladem o předání díla dle této smlouvy. Předávací protokol bude obsahovat řádné označení smluvních stran, jména a příjmení oprávněných osob smluvních stran, které předání a převzetí potvrdily, jejich podpisy, označení předávaného díla a veškerých písemných výstupů a datum podpisu předávacího protokolu.

7. Pokud Objednatel bezdůvodně odepře řádně a včas provedené dílo jeho převzít nebo požádá o posunutí termínu převzetí, není Zhotovitel v prodlení.
8. Podepsáním předávacího protokolu je zahájen proces akceptace díla. Objednatel má možnost ve lhůtě 2 kalendářních týdnů upozornit na zjištěné vady díla. Pokud tak Objednatel neučiní, považuje se dílo za akceptované.
9. Pokud Objednatel dílo neakceptuje, je povinen vystavit protokol o odmítnutí akceptace díla se specifikací důvodů odmítnutí. Pokud bude příčina na straně Zhotovitele, Zhotovitel zajistí, aby dílo odpovídalo požadavkům uvedeným v této smlouvě, a to ve lhůtě uvedené v protokolu o odmítnutí akceptace. Po provedení úprav díla se bude opakovat postup uvedený v odst. 4, 6 a 9 tohoto článku smlouvy, a to až do okamžiku akceptace díla. Při opakované akceptaci díla se lhůta pro uplatnění vad stanoví na 1 kalendářní týden od podpisu o předání upraveného díla.
10. Vlastnické právo k prováděnému dílu přechází na Objednatele okamžikem úhrady ceny díla. Zhotovitel nese odpovědnost za škody způsobené činností Zhotovitele nebo v souvislosti s ní jak na prováděném díle, tak na věcech k jeho provedení opatřených vč. prostor určených k provedení díla a přístupových cest, a to do dne převzetí řádně dokončeného díla Objednatelem.

Čl. IX
Odpovědnost za škodu

1. Smluvní strany odpovídají za škodu způsobenou porušením povinností vyplývajících z této smlouvy nebo z obecně závazného právního předpisu.
2. Případné poškození nedokončeného a/nebo nepřevzatého díla nese na svůj náklad Zhotovitel.

Čl. X
Licence

1. Ke všem částem díla, které mají povahu autorského díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „***autorský zákon***“), a k nimž Zhotovitel má nebo mu vznikne majetkové autorské právo, poskytuje Zhotovitel Objednateli licenci ke všem obvyklým způsobům užití díla známým ke dni uzavření této smlouvy, a to k užití díla Objednatelem, jako konečnými uživateli díla k účelu, k němuž dílo slouží, a to s účinností ode dne přechodu vlastnického práva k věci, v níž bylo konkrétní autorské dílo zahrnuto, nejpozději však ode dne dokončení díla.

2. Licenci dle předcházejícího odstavce této smlouvy Zhotovitel uděluje Objednateli za úplatu, která je součástí ceny díla, jako licenci nevýhradní, nepřenosnou na třetí osobu. Zhotovitel jménem autorů autorského díla uděluje Objednateli oprávnění k zapracování, sloučení nebo připojení autorských děl a jejich částí, dodaných Zhotovitelem dle této smlouvy, do systémů Objednatele dle potřeb a vůle Objednatele, a dále k jakýmkoliv změnám uvedených autorských děl, pokud jsou změny nezbytné k využití díla k jeho účelu, ke kterému má sloužit anebo k dosažení vzájemného funkčního propojení s jinými systémy Objednatele.

3. Zhotovitelem udělená licence se vztahuje ve shora uvedeném rozsahu i na jakékoli rozšíření, upgrady, updaty a další změny autorských děl, jsou-li dodány Zhotovitelem dle této smlouvy.

4. Zhotovitel se zavazuje učinit všechna nezbytná opatření nutná pro zabezpečení nerušeného výkonu práv vyplývajících z této smlouvy pro Objednatele.

5. Zhotovitel prohlašuje, že je oprávněn udělit licence a oprávnění uvedená v tomto článku. Pokud zhotovitel zjistí, že nebude moci dostát prohlášení dle předchozí věty, je povinen na takovou skutečnost Objednatele neprodleně písemně upozornit. Zhotovitel odpovídá Objednateli za jakoukoliv škodu, nemajetkovou újmu či náklady, včetně veškerých výdajů na odbornou právní pomoc, vyplývající z jakéhokoli porušení autorských a jiných práv duševního vlastnictví zhotovitele nebo třetích osob užíváním autorských děl dodaných zhotovitelem za účelem provedení díla.

Čl. XI
Bezpečnost informací

1. Zhotovitel je povinen dodržovat platnou legislativu ČR i EU, která se týká bezpečnosti informací.
2. Zhotovitel se zavazuje dodržovat požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele uvedené v příloze č. 3 této smlouvy.
3. Zhotovitel je povinen zajistit plnění bezpečnostních opatření a požadavků stanovených touto smlouvou ve stejné míře u všech případných poddodavatelů jiných osob, které mají přístup k informačním aktivům Objednatele prostřednictvím Zhotovitele.
4. Zhotovitel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které mu byly v souvislosti s touto smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi Zhotovitel seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění Zhotovitele veřejně přístupnými stanou (dále jen „důvěrné informace“). Zhotovitel nesmí důvěrné informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch Objednatele. Zhotovitel nesmí důvěrné informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch Objednatele. Zhotovitel se dále zavazuje zejména zajistit ochranu dat, které obsahují informace o osobních nebo citlivých údajích třetích osob –klientů atp., s nimiž přijde Zhotovitel (jeho zaměstnanci) do kontaktu v rámci plnění této smlouvy, a to v souladu s NAŘÍZENÍM EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), a v souladu se zákonem č. 110/2019 Sb., o zpracován osobních údajů, ve znění pozdějších předpisů, tzn. zejména zabezpečit, aby byla zachována mlčenlivost o těchto údajích, o všech bezpečnostních opatřeních, a aby zaměstnanci vyvíjeli snahu zabránit jakémukoliv zneužití těchto údajů jinou osobou. Povinnosti dle tohoto odstavce je Zhotovitel povinen zachovávat i po zániku této smlouvy, vyjma případů, kdy se důvěrné informace stanou prokazatelně veřejně přístupné bez zavinění Zhotovitele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je zhotovitel povinen zveřejnit důvěrnou informaci na základě povinnosti uložené Zhotoviteli právním předpisem nebo rozhodnutím orgánu veřejné moci.
5. Za nesplnění kterékoliv povinnosti obsažené v tomto článku, je Objednatel oprávněn účtovat Zhotoviteli smluvní pokutu ve výši 100 000 Kč, a to za každé jednotlivé porušení povinností obsažených v tomto článku.
6. Zhotoviteli na základě této smlouvy nevzniká žádné právo na užití dat zpracovávaných prostřednictvím díla.
7. Objednatel si vyhrazuje právo na provedení kontroly či auditu plnění vybraných požadavků/ustanovení u Zhotovitele. Za vybrané požadavky/ustanovení jsou považována tato:
    a. Kontrola/audit plnění požadavků specifikovaných v příloze č. 3 - Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele
    b. Kontrola/audit plnění požadavků specifikovaných v příloze č. 2 - Požadavky na bezpečnost webového portálu Kraje Vysočina v kapitole č. 5 Vývoj.

8. V rámci kontroly či auditu u Zhotovitele se Zhotovitel zavazuje poskytnout důkaz o plnění Objednatelem vybraného požadavku, a to buď fyzicky přímo v provozovně Zhotovitele, nebo vzdáleně pomocí elektronických prostředků.
9. Objednatel si vyhrazuje právo na informace o:
    a. významné změně ovládání Zhotovitele podle zákona o obchodních korporacích,
    b. změně vlastnictví zásadních aktiv Zhotovitele, které souvisejí s plněním této smlouvy,
    c. změně oprávnění nakládat s těmito aktivy.

Čl. XII
Smluvní pokuty, sankce

1. Při prodlení Objednatele s úhradou faktur činí úrok z prodlení 0,05 % z fakturované částky za každý den prodlení.
2. Pro případy neplnění věcných a termínovaných závazků vyplývajících z této smlouvy smluvní strany sjednávají tyto smluvní pokuty:
    2.1. Při prodlení Zhotovitele, pokud bylo prokazatelně způsobeno ze strany Zhotovitele, s prováděním nebo dokončením díla, resp. jeho dílčí etapy oproti termínům a lhůtám uvedeným v čl. III odst. 1 této smlouvy zaplatí Zhotovitel Objednateli smluvní pokutu ve výši 0,05 % z ceny díla sjednané touto smlouvou, resp. jeho dílčí etapy, u které je v prodlení, a to za každý i započatý den takového prodlení, maximálně však po dobu 30 dnů.
    2.2. Při prodlení Zhotovitele, pokud bylo prokazatelně způsobeno ze strany Zhotovitele, s dokončením díla, resp. jeho dílčí etapy přesahujícím lhůtu 30 dnů dle odst. 2.1 tohoto článku smlouvy, zaplatí Zhotovitel Objednateli smluvní pokutu ve výši 0,1 % z ceny díla sjednané touto smlouvou, a to za 31. a každý další i započatý den takového prodlení.
3. Pokud Zhotovitel poruší povinnosti stanovené čl. II. odst. 17 a v příloze č. 2 této smlouvy, je Objednatel oprávněn účtovat Zhotoviteli smluvní pokutu ve výši 50 000 Kč za každé jednotlivé porušení této povinnosti.
4. Pokud Zhotovitel neplní jiné povinnosti podle této smlouvy, je Objednatel oprávněn požadovat po Zhotoviteli a Zhotovitel je povinen zaplatit smluvní pokutu ve výši 1 000 Kč za každé jednotlivé porušení této smlouvy, za každý i započatý den prodlení.
5. Výše smluvních pokut dle odst. 1 a 2 tohoto článku nepřevýší cenu díla bez DPH dle čl. IV odst. 1 této smlouvy.
6. Smluvní pokuty dle tohoto článku jsou splatné do 15 kalendářních dnů od doručení písemné výzvy oprávněné smluvní strany povinné smluvní straně. Zaplacením smluvní pokuty nezaniká příslušný nárok oprávněné smluvní strany na splnění povinnosti povinné smluvní strany smluvní pokutou zajištěné. Smluvní pokuty se nezapočítávají na nárok na náhradu škody. Objednatel je oprávněn jednostranně započíst pohledávku na zaplacení jakékoli smluvní pokuty dle této Smlouvy na jakoukoli pohledávku Zhotovitele vůči Objednateli dle této Smlouvy.
7. Zaplacení smluvní pokuty nemá vliv na právo smluvních stran domáhat se náhrady škody vzniklé porušením smluvní povinnosti nebo povinnosti vyplývající z obecně závazného právního předpisu.
8. Škoda způsobená Objednateli poddodavatelem Zhotovitele se považuje za škodu způsobenou přímo Zhotovitelem.
9. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

10. Zhotovitel se nedostává do prodlení v případě prodlení Objednatele s poskytnutím nutné součinnosti Zhotoviteli (např. prodlení s umožněním přístupu do prostor, které jsou místem plnění).
11. Pokud Zhotovitel přeruší provádění díla, je povinen zajistit ochranu a bezpečnost pozastaveného díla proti zničení, ztrátě nebo poškození, jakož i skladování věcí opatřených k provádění díla.

Čl. XIII
Platnost, změna a zánik smlouvy

1. Tato smlouva nabývá platnosti dnem podpisu a účinnosti dnem zveřejnění v informačním systému veřejné správy – Registru smluv.
2. Platnost smlouvy lze ukončit písemnou dohodou podepsanou oprávněnými zástupci obou smluvních stran.
3. Objednatel má právo od této smlouvy odstoupit v případě, že:
    - Zhotovitel je v prodlení, pokud bylo prokazatelně způsobeno ze strany Zhotovitele, s prováděním či dokončením díla delším než 30 dní.
    - Zhotovitel vstoupí do likvidace nebo bude na jeho majetek prohlášen soudem konkurz nebo bude zamítnut návrh na vyhlášení konkurzu pro nedostatek majetku nebo zanikne bez likvidace a/nebo bude soudem prohlášen úpadek Zhotovitele a/nebo Zhotovitel vstoupí do insolvence.
    - Zhotovitel i přes upozornění Objednatele provádí dílo poddodavatelem v rozporu s čl. X této smlouvy.
    - Po uzavření smlouvy Objednatel zjistí, že smlouva neměla být uzavřena, neboť Zhotovitel před zadáním části veřejné zakázky předložil údaje a/nebo dokumenty, které neodpovídaly skutečnosti a měly nebo mohly mít vliv na výběr dodavatele.
    - dojde k významné změně ovládání Zhotovitele podle zákona o obchodních korporacích,
    - dojde ke změně vlastnictví zásadních aktiv Zhotovitele, které souvisejí s plněním této smlouvy,
    - nebo dojde ke změně oprávnění Zhotovitele nakládat s těmito aktivy.
4. Kterákoliv smluvní strana má právo odstoupit od této smlouvy i z kteréhokoliv zákonného důvodu.
5. Odstoupení je účinné doručením písemného oznámení o odstoupení druhé smluvní straně.
6. Obsah této smlouvy může být měněn jen dohodou smluvních stran, a to vždy jen vzestupně číslovanými písemnými dodatky podepsanými oprávněnými osobami smluvních stran.

Čl. XIV
Závěrečná ustanovení

1. Výběr Zhotovitele byl proveden v souladu se zákonem a Pravidly Rady Kraje Vysočina pro zadávání veřejných zakázek ze dne 29. 6. 2021.
2. Zhotovitel prohlašuje, že se před uzavřením smlouvy nedopustil v souvislosti s veřejnou zakázkou sám nebo prostřednictvím jiné osoby žádného jednání, jež by odporovalo zákonu nebo dobrým mravům nebo by zákon obcházelo, zejména že nenabízel žádné výhody osobám podílejícím se na zadání veřejné zakázky, na kterou s ním Objednatel uzavřel tuto smlouvu, a že se zejména ve vztahu k ostatním dodavatelům nedopustil žádného jednání narušujícího hospodářskou soutěž.
3. Vzhledem k veřejnoprávnímu charakteru Objednatele Zhotovitel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním smluvních podmínek obsažených v této smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů, zejména zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

4. Není-li v této smlouvě výslovně uvedeno jinak, právní vztahy smluvních stran touto smlouvou blíže neupravené se řídí příslušnými ustanoveními občanského zákoníku, jakož i dalšími obecně závaznými právními předpisy ČR.
5. Tato smlouva se vyhotovuje elektronicky, přičemž každá smluvní strana obdrží originální vyhotovení smlouvy podepsané zaručenými či uznávanými elektronickými podpisy osob oprávněných za ně jednat.
6. Zhotovitel výslovně souhlasí se zveřejněním celého textu této smlouvy včetně podpisů v informačním systému veřejné správy – Registru smluv.
7. Smluvní strany se dohodly, že zákonnou povinnost dle § 5 odst. 2 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), splní Objednatel a splnění této povinnosti doloží Zhotoviteli. Smluvní strany současně berou na vědomí, že v případě nesplnění zákonné povinnosti je smlouva do tří měsíců od jejího podpisu bez dalšího zrušena od samého počátku.
8. Nedílnou součástí této smlouvy je:
   - příloha č. 1 –Technická specifikace a harmonogram,
   - příloha č. 2 – Požadavky na bezpečnost webového portálu Kraje Vysočina
   - příloha č. 3 – Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele

   Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly, s jejím obsahem souhlasí, že smlouva je v souladu s jejich svobodnou vůlí a smlouvu nepodepisují v tísni a za nápadně nevýhodných podmínek. Na důkaz toho připojují své podpisy.

V Jihlavě

Ing. Jitka Savická
Digitálně podepsal Ing. Jitka Savická
Datum: 2022.04.19 14:40:03 +02'00'

za Zhotovitele
Ing. Jitka Savická
Jednatelka společnosti

V Jihlavě

RNDr. Jan Bříždala
Digitálně podepsal RNDr. Jan Bříždala
Datum: 2022.04.25 09:03:53 +02'00'

za Objednatele
RNDr. Jan Bříždala
Radní kraje

Příloha č. 1 - Technická specifikace a harmonogram

Navrhovaný harmonogram

1. **Návrh designu nového webu a prvků - 04-05/2022**
   a. Typ dokumentu (článek, aktualita, příloha, právní předpis, úřední deska, kalendář akcí, osoba - telefonní seznam)
   b. **(X2** – viz specifikace níže**)** Dlaždice (grafické, textové)
   c. **(X3)** Štítky (pro filtrování, hledání, související články, kalendář akcí)
   d. **(X5)** Články, výpis článků, filtrování
   e. **(X6)** Kalendář akcí
   f. text + obrázek, text + dlaždice, text + odkazy (vlevo-vpravo)
   g. Accordion, záložky

2. **Funkční prototyp (05-06/2022)**
   a. Full responzive, orientované na mobilní zařízení
   b. Webová prezentace musí být zcela přístupná i pro osoby s různou úrovní handicapu využívající k prohlížení webu specializované nástroje. Při tvorbě nového webu musí být splněny veškeré požadavky zmíněné v zákoně č. 99/2019 Sb. o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.
   c. Příklady použití prvků ve vzorových stránkách
      1. **(X2)** Dlaždice (grafické, textové)
      2. **(X3)** Štítky
      3. **(X5)** Články

3. **Testovací instance Vismo (07-08/2022) – pro naplnění základní struktury webu**
   a. Tvorba složek a základních dokumentů
   b. Tvorba portálků
   c. **(X3)** Štítky (pro filtrování, hledání, související články, kalendář akcí)
   d. text + obrázek, text + dlaždice, text + odkazy (vlevo-vpravo)

4. **Integrační úlohy I. (09-10/2022)**
   a. Načítání telefonního seznamu
   b. **(X6)** Napojení kalendáře akcí

5. **Nasazení ostré instance Vismo – 10-11/2022**
   a. Hezká URL, možnost nastavit vlastní
   b. **(X1)** Vyhledávání s našeptávačem
   c. **(X7)** Úřední deska včetně JSON pro NKOD
   d. Převod do PDF na pozadí
   e. **(X5)** Hromadné nahrávání obrázků, příloh, hromadné operace s nimi - např. přejmenování
   f. Jazykové mutace (možnost mít jiné stromy v různých mutacích)
   g. Mapa webu
   h. Tiskový pohled všech stránek s možností přímého tisku do PDF
   i. Dodavatel provede přesměrování URL adres z původního webu kraje na úrovni webového serveru s nasměrováním na nové složky na základě mapy starého webu (URL adres) na strukturu nového webu včetně nástroje na správu těchto vazeb
   j. Multi domain systém (možnost v rámci webu mít více subprojektů s jinou doménou), možnost jiné grafiky
   k. Accordion, záložky

l. rich text (volba počtu sloupců), nebo více předvoleb (např. vlevo richtext a vpravo dlaždice, bannery, fotogalerie odkazy apod.)

6. **Integrační úlohy II (01-06/2023)**
   a. IDM oprávnění skupiny a napojení na skupinu oprávnění SAML2 autentizaci prostřednictvím Shibboleth - https://vysocinaid.kr-vysocina.cz/
   b. **(X12)** Exportní nástroje
   c. RSS

7. **Výhledové úlohy (06-12/2023)**
   a. **(X10)** Odběr novinek
   b. **(X4)** Číselníky
   c. **(X8)** Zobrazení map, pokročilé filtrování
   d. **(X12)** Exportní nástroje
   e. Zobrazení PDF integrované ve stránce (ISSUU)
   f. **(X9)** Formulářový systém
   g. Vložení odkazů na související článek do textu?
   h. **(X11)** Speciální objekt "Seznam" pro datově založené projekty
   i. Optimalizace pro rychlost načítání a vyhledávání (cache, předgenerování,....atp.)

Podrobnější popis:

- **(X1) Vyhledávání s našeptávačem a rozšířeným filtrováním**
  - našeptávač
  - typ (úřední deska, kontakt, článek, příloha, kalendář akcí, číselník, právní předpis, fotogalerie)
  - štítky
  - Fulltextové vyhledávání v přílohách (DOCx, PDF, XLS, PPT,...)
  - Vyhledávání i v telefonním seznamu
  - Widget Volitelné Vyhledávací pole v podsekci, kde se uživatel nachází (dvě vyhledávací pole jedno globální, druhé lokální)

- **(X2) Dlaždice (grafické, textové)**
  - použitelné na více místech s určením pořadí
  - ikona (inverzní zabarvení při přejetí myši) + text
  - obrázek + text dole
  - ikona vlevo + text vpravo
  - textové

- **(X3) Štítky**
  - Víceslovné štítky (délka několik slov)
  - Filtrovaní
  - vyhledávaní
  - Našeptávač
  - Na základě štítků řešit související články
  - Kalendář akcí (jiná sada štítků načtená z WS kalendáře akcí)
  - definované sady nebo skupiny štítků pro různé použití (např úřední deska, kalendář akcí, články,...)

- **(X4) Číselníky**
  - viz dědictví
  - Filtrování a vyhledáváni

    - Možnost administrátorsky vytvořit číselník a ten pak používat jako typ sloupce, nebo metadat (např u typu seznam, nebo u článků)

- **(X5) Články**
    - typy článku (různé vizuální podoby, dle počtu příloh, map, přítomnosti textu)
    - fotogalerie + videa
    - Fotogalerie rozbalovat přímo do stránky bez znovunačtení
    - **Štítky (X4)**
    - Související články - automaticky + ručně
    - Možnost zobrazit článek na jiném místě webu v jiné složce (navigace dle primárního umístění)
    - možnost vložit pod článek další widgety
    - možnost nastavit další metadata v dané sekci
    - Hromadné nahrávání obrázků, příloh, hromadné operace s nimi - např. přejmenování

- **(X6) Kalendář akcí**
    - načítání z kalendáře + možnost vložit ručně
    - Štítky (načítané z číselníků, přes WS, a možnost ručního přidání)
    - filtry dle data místa vzdálenosti a štítků
    - Možnost vložit souřadnici a zobrazit mapu
    - widget s ručním výběrem akce nebo sekce dle štítků

- **(X7) Úřední deska**
    - samostatná složka a samostatný typ článku
    - štítky pro kategorizaci **(X4)**
    - zobrazení Stav ke dni (archiv úřední desky)
    - uživatelsky nesmazatelné
    - Zveřejnění na eÚD provádí určená osoba
    - Json pro NKOD

- **(X8) Mapy**
    - seznamu bodů a ploch a načítání obrázku. načítání z dat přes WS a DB

- **(X9) Formulářový systém**
    - uložení do DB + mail
    - Umožňuje vkládat tyto předdefinované pole
        - textové pole
        - textové pole (dlouhý text s možností formátování)
        - combo box
        - zaškrtávací pole s možností více výběrů (check box)
        - výběrové pole 1 z N (radio button)
        - příloha"
    - Ochrana formuláře pomocí RECAPTCHA ve verzi 3

- **(X10) Odběr novinek**
    - sledování frází
    - Sledování dle
        - Štítků
        - sekce menu
        - Složky
        - Typ dokumentu
    - denně/týdně/měsíčně

- **(X11) Speciální objekt "Seznam" pro datově založené projekty**

- Název
- volba parametrů (nastavení typů a názvů sloupů)
- vyber číselníku + možnost zobrazit v rozšířeném vyhledávaní
- číselníky a souřadnice pro mapy.
- Obrázky (vlastní ikony) do map
- Možnost stromového filtrování na začátku několik možností rozpad na další filtry **pro seznam skol** (např http://dedictvivysociny.cz/, nebo https://www.vyberskoly.cz/online#1|26|O4|BR|11|637389377086184667180921 38)
- Univerzální import dat např. https://pimcore.com/docs/data-importer/current/#_

- **(X12) Univerzální exportní nástroj obsahu**
  - Možnost definovat která část webu bude obsahem exportu (např json.)
  - Možnost definice na základě složky (včetně podsložek), typu dat, štítků,

- **Vizuální prvky (widgety)**
  - Volitelné Vyhledávací pole v podsekci, kde se uživatel nachází (dvě vyhledávací pole jedno globální, druhé lokální)
  - Volitelné vypnuti menu
  - **(X2)** Dlaždice (použitelné na více místech s určením pořadí)
  - **(X5)** Výpis článku zobrazení sekce dokumentů (s obrázky a bez), možnost konfigurace, která část stromu se zobrazuje
  - **(X2)** tabulka Odkazy + ext odkazy automaticky označeny ikonou (textové dlaždice)
  - **(X6)** Kalendář akci z WS + štítky (možnost zobrazit jen sekce, nebo dle štítku)
  - Accordion pro další widgety viz tlf. Seznam.
  - Definovatelné záložky s dalším obsahem
  - text + obrázek, text + dlaždice, text + odkazy (vlevo-vpravo)
  - rich text (volba počtu sloupců), nebo více předvoleb (např. vlevo richtext a vpravo dlaždice, bannery, fotogalerie odkazy apod)
  - Banner s odkazy (forma dlaždic)
  - **(X8)** Mapy (možnost vložit mapku s bodem, nebo seznamem bodů viz datový typ seznam)
  - Zobrazení fotogalerie
  - Slider obrázků
  - bannery
  - **(X9)** Nastavitelný formulář
  - **(X11)** Seznam záznamu s definování sloupci - rozšířené metadata k článkům

Cenová kalkulace		
	Cena v Kč bez DPH	**Cena v Kč s DPH**
Tvorba stránek se systémem vismo Online – 1. fáze, rok 2022	500 000 Kč	605 000 Kč
Tvorba stránek se systémem vismo Online – 2. fáze, rok 2023	400 000 Kč	484 000 Kč

Příloha č. 2 - Požadavky na bezpečnost webového portálu Kraje Vysočina

WWW stránky kraje jsou identifikovány jako **významný informační systém** podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících právních předpisů. Níže jsou uvedeny požadavky na webový portál Kraje Vysočina včetně všech komponent a infrastruktury (dále jen systém nebo informační aktivum) tak, aby systém naplňoval požadovanou úroveň kybernetické a informační bezpečnosti dle:

- zákona č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících právních předpisů,
- dobré praxe
- aktuálních bezpečnostních potřeb zadavatele.

Logování a auditní záznamy

Systém musí splňovat následující požadavky v oblasti logování a auditních záznamů. Tyto požadavky jsou v souladu s vyhláškou o kybernetické bezpečnosti v platném znění.
Jedná se o základní požadavky na strukturu, formát, obsah, protokol a technickou konfiguraci auditních záznamů a logů jednotlivých prvků systému tak, aby měly tyto informace vypovídající hodnotu pro řešení a forenzní analýzu kybernetických bezpečnostních událostí a aby byly jednoduše integrovatelné na centrální nástroj pro sběr a analýzu těchto dat.

Obsah auditních záznamů a logů

Auditní záznamy a logy systému musí obsahovat minimálně tyto informace:

- přihlášení a odhlášení všech uživatelů (včetně administrátorů či jiných privilegovaných účtů),
- činnosti prováděné uživateli,
- činnosti provedené administrátory, např. (pokud danou funkcionalitu obsahují):
    - přidělení/odebrání oprávnění,
    - založení/smazání uživatele,
    - přidělení/odebrání role,
    - reset hesla (pokud je prováděn na úrovni logujícího informačního aktiva),
    - povýšení oprávnění administrátora, převzetí role konkrétního uživatele,
    - změna konfigurace logování událostí,
    - změna konfigurace informačního aktiva,
- automatická informační, varovná a chybová hlášení provozního charakteru (tzv. aplikační a systémové logy),
- požadavky o přístup k jednotlivým stránkám.

Osobní údaje

Pokud jsou v informačním aktivu zpracovávány osobní údaje (nebo osobní údaje zvláštní kategorie, tzv. citlivé osobní údaje), mezi minimální požadavky na auditní záznamy a logy patří rovněž tyto informace:

- Činnosti uživatelů týkající se osobních údajů/osobních údajů zvláštní kategorie:

    - prohlížení údajů,
    - editace/zápis údajů,
    - mazání údajů.

Struktura auditních záznamů a logů

Auditní záznamy a logy musí obsahovat minimálně tyto parametry a metadata:

- identifikátor události,
- identifikátor zdroje událostí,
- přesné datum vzniku události,
- přesný čas vzniku události včetně specifikace časového pásma,
- typ/název události,
- případně popis události (pokud není zřejmé z typu/názvu),
- jednoznačnou identifikaci účtu, pod kterým byla událost provedena,
- jednoznačnou síťovou identifikaci zařízení původce a
- úspěšnost nebo neúspěšnost (včetně neprovedení činnosti v důsledku nedostatečných oprávnění) události.

Formát auditních záznamů a logů

Formát (resp. standard) logů musí být v jedné z následujících možností:

- syslog (RFC 5424) + syslog over TLS,
- 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 zadavatelem), např.:
    - json,
    - plain-text line-oriented logy,
    - xml,
    - atd.

Úrovně auditních záznamů a logů

Informační aktivum musí zaznamenávat auditní záznamy a logy na všech existujících úrovních – tj. na úrovni

- operačního systému,
- aplikačního serveru/modulu (např. web server, sql server, apod.),
- i na úrovni samostatné aplikace/informačního systému/služby informačního systému.

AAA

Systém musí splňovat následující požadavky v oblastech autentizace, autorizace a accountingu.

Autentizace

Systém musí umožňovat autentizaci vůči:
- Externímu zdroji identit
- Internímu zdroji identit

Požadavky na autentizaci vůči externímu zdroji identit:

Pro autentizaci vůči externímu zdroji identit (Shibboleth) musí být použit zabezpečený protokol (HTTPoverSSL), který splňuje požadavky na kryptografii, které jsou definované dále v této zadávací dokumentaci.

Požadavky na autentizaci vůči internímu zdroji identit:

Systém musí umožnit nadefinování vlastní heslové politiky pro jednotlivé typy lokálních (záložních) účtů, a to minimálně v tomto rozsahu:
- stáří hesla,
- granulární komplexita hesla (určení kategorií znaků),
- délka hesla,
- historie hesla (počet opakování).

Uložení hesel v DB musí být v souladu s požadavky na kryptografii, které jsou definované dále v této zadávací dokumentaci.

Autorizace

Systém musí umožňovat granulární řízení přístupových oprávnění na základě aplikačních rolí.
V případě autentizace vůči externímu zdroji identit musí být přidělování přístupových oprávnění (aplikačních rolí) založeno na uživatelských skupinách.
Úrovně všech přístupových oprávnění/jednotlivých rolí musí být detailně popsány (např. formou popisu role v administračním rozhraní a v dokumentaci systému).
Aplikační servery/moduly (např. web server, DB server, apod.) nesmí vyžadovat pro své spuštění privilegovaná oprávnění (např. typu root, Administrator, NT Authority\System, sysadmin, apod.). Tato privilegovaná oprávnění nesmějí být vyžadována pro běh zmíněných částí systému v průběhu implementaci či provozu systému.

Accounting

Každý uživatel systému musí být unikátní (musí mít jednoznačný identifikátor) a personifikovaný.

Nesmí existovat sdílený uživatel či sdílené heslo pro více uživatelů.
V případě potřeby použití účtu typu "super administrátor" (privilegovaný uživatel s možností převzít na sebe roli někoho jiného) je nutné dodržovat tato pravidla:

- použití jiného uživatele prostřednictvím "superadministrátora" musí být zaznamenáno v auditní stopě
- všechny operace provedené superadministrátorem musí být logovány
- superadministrátor musí být v systému zaveden formou role (nikoliv 1 uživatelského účtu), kterou lze přiřadit

Přenos dat

Systém musí splňovat následující požadavky na přenos dat.
Přenos dat musí probíhat vždy pomocí zabezpečeného protokolu, např. HTTPS, SSH, sFTP, SCP, LDAPoverTLS, SAML2.0, Radius, apod.).
Informační aktivum musí umožňovat přenos dat do sítě Internet přes aplikační HTTP proxy, která je systémově nastavená (případně lze konfigurovat přímo v aplikaci).
Uchazeč musí při implementaci systému vyspecifikovat všechny potřebné zdroje ze sítě Internet, které jsou nezbytné pro provoz systému za účelem vytvoření tzv. white-listu na aplikační HTTP proxy.

Kryptografie

Systém musí naplňovat níže uvedené minimální požadavky na kryptografii, které vychází z aktuální best practise a z doporučení NÚKIB.

Obecně

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

Hashovací funkce

Ukládání otisků hesel

- pro ukládání hesel uživatelů mohou být použity pouze tyto tzv. pomalé hashovací funkce:
  - Argon2i
  - bcrypt
  - scrypt
  - PBKDF2
- 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.

Elektronické podepisování e-mailů a dokumentů

- SHA-2 a vyšší
- délka otisku 256 bitů a vyšší

Ověřování integrity souborů

- SHA-2 a vyšší
- délka otisku 224 bitů a vyšší

Asymetrická kryptografie

SSL/TLS

- 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) - 2048 bitů a více (postupně přecházet na 3072 bitů, tam kde to bude možné)
            - 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 - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
            - 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
    - Způsob naplnění:
        - Diffie-Hellman implementace: https://weakdh.org/sysadmin.html
- Certifikáty dodá zadavatel
- Systém musí respektovat a umožnit použití TLS systémových certifikátů v modelu využívajícím webový aplikační FW, kdy:
    - Interní uživatelé přistupující k webovému rozhraní v rámci LAN identifikují server pomocí TLS systémového certifikátu vystaveného pomocí interní certifikační autority
    - Externí uživatelé přistupující k webovému rozhraní z DMZ/Internetu identifikují server pomocí TLS systémového certifikátu vystaveného pomocí veřejné certifikační autority
    - WAF v rámci komunikace s externími klienty předkládá TLS systémový certifikát vystavený veřejnou certifikační autoritou, ale v roli klienta navazuje komunikace s webovým rozhraním pomocí interního certifikátu
-

Šifrování, podepisování a autentizace

- týká se různých technologií PKI, PGP, S/MIME, SSH, apod.
- minimální délka klíče
    - algoritmus DSA – 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
    - algoritmus RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
    - algoritmus ECDSA - 256 bitů
- Ověřování (např. SSH klíče)
    - délka klíče minimálně 2048 bitů u RSA a DSA algoritmů (postupně přecházet na 3072 bitů, tam kde to bude možné)
    - délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky

Symetrická kryptografie

- nesmí být použity tyto šifry:
    - DES, 3DES, RC4, Blowfish, Kasumi
- minimální délka šifrovacího klíče - 128 bitů
    - pro šifru Chacha20 minimálně 256 bitů a se zatížením klíče menším než 256 GB
- nesmí být použity tyto módy pro ochranu integrity:
    - HMAC-SHA1, CBC-MAC-X9.19

HTTP Headers

Webový server musí být nakonfigurován tak, aby zajišťoval maximální možnou míru informační bezpečnosti a naplňoval minimálně následující požadavky na bezpečnostní http hlavičky:

- X-Frame-Options

    - Musí být implementována (tzn. server ji musí klientské aplikaci zasílat) – v odůvodněných případech může být vynechána.
    - Záhlaví může nabývat pouze hodnot DENY nebo SAMEORIGIN dle potřeby
- Strict-Transport-Security
    - Musí být implementována
    - Direktiva max-age musí nabývat hodnoty minimálně 31536000
    - Ostatní direktivy jsou volitelné
- Content-Security-Policy
    - Musí být implementována
    - Nesmí obsahovat direktivy unsafe-inline, unsafe-eval
    - Aktiva mohou být načítána pouze prostřednictvím zabezpečeného protokolu (direktiva https:)
    - Aktiva mohou být načítána pouze z konkrétních a bezpečných zdrojů
    - Pokud by bylo nutné načítat aktiva z jiných zdrojů, které nejsou umístěny na infrastruktuře, která je v držení Kraje Vysočina nebo dodavatele, podléhají tyto zdroje nejprve schválení Krajem Vysočina. Pokud ke schválení Krajem Vysočina nedojde, tyto zdroje nemohou být použity k načítání aktiv spolu se zbytek webové stránky
- X-Content-Type-Options
    - Musí být implementována
- Referrer-Policy
    - Musí být implementována
    - Nesmí obsahovat direktivy: prázdný string, unsafe-url
- Permissions-Policy
    - Musí být implementována
    - Mohou být povolena pouze ta oprávnění, která jsou skutečně potřeba, všechna ostatní musí být explicitně zakázána
- X-XSS-Protection
    - Musí být implementována
    - Directiva politiky musí nabývat hodnoty 1; mode=block
- Server
    - Pokud je hlavička implementována, musí být změněna tak, aby neodhalovala citlivé informace odhalující verzi webového serveru
- Set-Cookie
    - Pokud se jedná o session cookies, musí obsahovat direktivu nastavující secure a httponly flagy.
- Cross-Origin-Embedder-Policy
    - Musí být implementována
- Expect-CT
    - Musí být implementována
- Cross-Origin-Opener-Policy
    - Musí být implementována
- Cross-Origin-Resource-Policy

- Musí být implementována

Vývoj

V rámci vývoje systému musí být zpracovávána bezpečnostní specifikace, která bude uchazečem předána v rámci bezpečnostně provozní dokumentace (viz. dále požadavky na bezpečnostně provozní dokumentaci.
Dále musí systém splňovat níže uvedené bezpečnostní požadavky na vývojové prostředí.
Ochrana před škodlivým kódem musí být zajištěna:

- na pracovních stanicích vývojářů a programátorů,
- na serverech/zařízení, kde je uložen zdrojový kód aplikací.

Ke zdrojovým kódům musí být řízen přístup tak, aby k němu měli přístup pouze oprávnění vývojáři a jiné oprávněné osoby uchazeče systému.
Přístupy ke zdrojovým kódům systému a jejich změny musí být monitorovány a logovány, auditní stopa přístupů musí být vyhodnocována. Pro správu zdrojového kódu musí být použit tzv. verzovací systém.
Zdrojové kódy systému musí být pravidelně zálohovány a zálohy pravidelně testovány na jejich obnovitelnost.
Zadavatel si vyhrazuje právo prověření naplnění těchto požadavků.

Oddělení prostředí

Systém musí být nasazen v prostředí zadavatele ve dvou oddělených prostředích: testovací a provozní.
Testovací prostředí musí splňovat tyto požadavky:

- může být pouze dočasné pro účely otestování aplikace (např. z pohledu akceptačních testů, odladění systému v ICT prostředí KrÚ, apod.) a školení uživatelů/administrátorů,
- v případě dočasného prostředí, musí být určeno, kdy může dojít k přechodu z testovacího do provozního prostředí (např. po splnění akceptačních testů, po schválení objednatelem, apod.),
- v případě trvalého testovacího prostředí musí být určeno, jakým způsobem bude odděleno (např. v názvu serveru bude uvedeno, že se jedná o test, odlišné umístění v síti, apod.).

Analýza rizik

Zadavatel se zavazuje k provedení podrobné a komplexní analýzy rizik informační bezpečnosti v souvislosti jak s nasazením systému, tak i s provozem tohoto systému. Analýza rizik informační bezpečnosti musí být zpracována před nasazením do provozního režimu. Zhotovitel/dodavatel vypracuje a předá objednateli:

- zdokumentovaný postup provedení analýzy rizik (metodiku, jak postupoval),

- zprávu z analýzy rizik obsahující vydefinovaná a klasifikovaná rizika, která jsou určena na základě míry dopadu, pravděpodobnosti výskytu zranitelnosti a pravděpodobnosti naplnění hrozby,
- popis těchto rizik,
- plán zvládání rizik s návrhy opatření na snížení míry případných rizik včetně popisu způsobu jejich nasazení.

Zadavatel bude schvalovat výstupy z provedené analýzy rizik před nasazením systému do provozního režimu.

Bezpečnostní testy

Objednatel provede bezpečnostní testy informačního aktiva s cílem ověření, zda není možné:

- získat neoprávněný přístup k službám/datům/systémům objednatele prostřednictvím informačního aktiva,
- neoprávněně modifikovat/zničit data objednatele prostřednictvím informačního aktiva,
- narušit dostupnost služeb/systémů objednatele prostřednictvím informačního aktiva,
- získat autentizační údaje uživatelů objednatele prostřednictvím informačního aktiva,
- zneužít infrastrukturu objednatele k útokům na sítě a služby třetích stran prostřednictvím informačního aktiva.

Testy budou provedeny před nasazením informačního aktiva do provozního režimu.
Výstup z těchto testů bude aplikován do akceptačních testů, kdy dílo nebude akceptováno v případě, že bude obsahovat zranitelnosti ohodnocené jako střední a kritické, tedy dosáhnou base score 4.0 až 10.0 dle otevřeného standardu hodnocení zranitelností CVSSv3.1 (Common Vulnerability Scoring System).

Bezpečnostně provozní dokumentace

Zhotovitel musí k systému dodat bezpečnostně provozní dokumentaci v rozsahu a oblastech určených níže.
Cílem zpracování této dokumentace je popsat a zdokumentovat provozní postupy pro zajištění správného, bezchybného a bezpečného provozování systému.

Bezpečnostní specifikace systému

Cíl dokumentu: popsat a zdokumentovat veškeré bezpečnostní mechanizmy a opatření za účelem identifikace toho, jaká data jsou jakým způsobem chráněna.
Forma dokumentu: textový popis, buď dle metodiky ITSEM (Information Technology Security Evaluation Manual podle ITSEC) nebo v rozsahu minimálně dle následujících bodů.
Minimální rozsah:

- Soupis a popis všech funkcí prosazujících bezpečnost pro:
    - Zajištění integrity dat při jejich přenosu a uložení
    - Zajištění důvěrnosti dat při jejich přenosu a uložení
    - Zajištění autentizace a session managementu
    - Zajištění ošetření, filtrování a prověřování vstupních dat
    - Zajištění auditní stopy a logování
    - Externí rozhraní – jak uživatelská, tak pro komunikaci s externími systémy
- Popis těchto oblastí:
    - Použité kryptografické funkce a algoritmy – popis přesné specifikace a použitých parametrů (typ funkce, délka klíče, mód šifrování, počet iterací, apod.)
    - Poloformální popis všech nestandardních algoritmů, funkcí a protokolů v oblasti bezpečnosti (např. vlastní šifrovací algoritmus, vlastní komunikační protokol, apod.)
    - Autentizační a autorizační model a mechanizmus (např. fáze autentizace, způsoby ověření, heslové politiky, protokoly, ...)
    - Řízení uživatelských a privilegovaných rolí a oprávnění (včetně Access Control, Least Priviledge principy, Multi-factor autentizace, Segregation of Duties principy, Accountability principy)
        - To vše z pohledu:
            - Interních uživatelů
            - Externích uživatelů
    - Detailní popis úrovně všech přístupových oprávnění/aplikačních rolí
    - Vývoj systému – použité bezpečnostní metodiky, praxe, frameworky, standardy a politiky při návrhu, plánování a vývoji systému
    - Způsob bezpečnostního testování systému
    - Monitoring řešení a zaznamenávání logů a auditní stopy (viz. část provozně bezpečnostní dokumentace Monitoring)
    - Způsob zajištění dostupnosti, důvěrnosti a integrity dat ve stavech jejich uložení/uchování, zpracování a přenosu
    - Soulad s právními normami pro ochranu osobních údajů
    - Bezpečnostní architektura infrastruktury systému
    - Bezpečnostní architektura klienta/koncového zařízení
    - Disaster recovery plán a strategie zálohování
    - Popis způsobu ošetření aplikace dle OWASP Testing guide v aktuální verzi.

Instalace systému

Cíl dokumentu: popsat a zdokumentovat postupy, kroky a činnosti vedoucí k instalaci systému nebo k přípravě prostředí pro instalaci.

- Forma dokumentu: textová, může být doplněno o návodné obrázky

- Systémové požadavky (architektura procesoru, verze operačního systému, minimální požadavky na výkon HW, apod.)
- Instalační média (CD, síť, soubor, …) a cesta k nim
- Konkrétní kroky vedoucí k instalaci systému, způsob instalace serverové části, způsob instalace klientské části, apod.

Základní konfigurace

Cíl dokumentu: popsat a zdokumentovat postupy, které vedou k nastavení systému do takového stavu, aby bylo možné systém po instalaci provozovat na základní úrovni.

- Forma dokumentu: textový popis (může být i např. formou okomentovaného config souboru)
- Základní konfigurace sítě (nastavení ip adresy, masky, GW, ...)
- Nastavení připojení/komunikace na další systémy (např. DB, web server, SMPT, DNS, NTP, ...), nastavení portů na kterých služba naslouchá, kam data odesílá, …
- Nastavení proxy pro komunikaci, seznam URL (nebo domén), kam systém potřebuje komunikovat (směrem do Internetu), ...
- Spuštění potřebných modulů, registrování knihoven, úprava registrů OS Windows, …
- Nastavení automatických úloh, nastavení systémových účtů, …
- Nastavení potřebných serverů (SMPT, DNS, NTP, ...)
- Detailní popis úrovně přístupových oprávnění/aplikačních rolí

Způsob zpracování informací

Cíl dokumentu: popsat, jakým způsobem jsou zpracovávány informace v rámci systému + případně v rámci ostatních systémů, na které je daný IS navázán.

- Forma dokumentu: textový popisu nebo i schéma
- Vytváření dat (datové vstupy)
    - manuálně|strojově|automaticky|uživatelsky
    - kdy jsou data vytvářena? (např. nějaká událost, naplánovaná událost, apod.)
    - …
- Přenosy dat

    - Odkud kam (např. agent>master, do jiných systémů, mezi moduly, apod.)?
    - Jakým protokolem?
- Uložení dat
    - Databáze (typ?) + cesta
    - File (typ?) + cesta
    - …
- Výstupy systému (dat)
    - User Interface (webový formulář, GUI aplikace, konzole, …)
    - E-mail|sms|voice call
    - Soubor (formáty)?
    - Tisk
    - Datová pumpa
    - Do jiných systémů (jakých?)

Záloha, obnova, restart

Cíl dokumentu: popsat a zdokumentovat strategii zálohování systému, jakým způsobem, kdy, kam a jak často jsou zálohována data v rámci daného systému a jakým způsobem se provádí obnova systému po havárii nebo ze zálohy, postupy a konkrétní kroky, které povedou k bezpečnému restartu systému.

- Forma: může být i formou zálohovacího plánu (backup schedule), textový popis
- Zálohování
    - Strategie zálohování systému navržená dodavatelem
    - Způsob zálohování – plná, přírůstková, rozdílová záloha
    - Kdy a jak často je záloha prováděna
    - Jak dlouhou dobu jsou zálohy uloženy a kde
    - Jak často se provádí testování záloh
- Obnova
    - Posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému nebo jeho části či dat ze zálohy do jeho plně funkčního stavu

- Zpracovaný disaster recovery plán, tedy posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému po jeho selhání do jeho plně funkčního stavu

- Restart
  - Posloupnost kroků (co a jak udělat), které je třeba provést pro bezpečné restartování systému tak, aby naběhl do původního stavu
    - Např. informování uživatelů, ověření odhlášení všech uživatelů, provedení zálohy systému, restart systému (konkrétní procesy, služby, apod.), způsob základní kontroly funkčnosti, informování uživatelů, výčet služeb, které je potřeba spustit/zkontrolovat, apod.

- Typicky způsob obnovy ze zálohy, popsání scénáře, apod.

Postupy řešení problémů

Cíl dokumentu: popsat, jakým způsobem se řeší případ nějakého problému, typicky nefunkčnost systému, nefunkčnost části systému, chybové stavy, základní troubleshooting, apod.

- Základ dokumentace: kontakty (e-mailové adresy, telefonní čísla, url helpdesku)
- V jakém případě, koho a prostřednictvím čeho (e-mailu, helpdesku, sms, telefonu) kontaktovat a jakým způsobem
- Základní troubleshooting
- Chybové stavy

Vazby na jiné systémy, rozhraní, datové vztahy a struktury

Cíl dokumentu: popsat, jakým způsobem je daný systém navázán na jaké systémy, popsat všechna rozhraní (např. uživatelské) a popsat datové vztahy a struktury.

- Forma: textový popis doplněný o schéma
- Výčet systémů, na jaké je daný systém navázán (DB, aplikační servery, fileservery, UI, pracovní stanice, zdroje informací /vstupy/, výstupy, datové pumpy, jiné IS, apod.)
- Komunikační protokoly (příp. rozhraní) připojení na jiné systémy
- Porty, ip adresy, identifikátory NIC, API
- Schéma datových toků
- Schéma datových toků osobních údajů, osobních údajů zvláštních kategorií a jiných citlivých informací

- Forma a struktura dat, způsob přenášení dat (použité protokoly), toky dat z a do kterých systémů, způsob jejich uložení, apod.
- Naplánované úlohy přenosu dat (např. datové pumpy), apod.
- Forma a struktura dat, obecný popis dat

Monitoring

Cíl dokumentu: popsat a zdokumentovat mechanizmus monitorování a zaznamenávání bezpečnostních a provozních logů a auditních událostí.

- Popis logů informačního aktiva
    - Výčet a popis všech událostí, které jsou zaznamenávány (př. přihlášení/odhlášení uživatele, provozní/chybové stavy, přidělení/odebrání oprávnění, …)
        - Včetně jejich jednotlivých identifikátorů
        - Včetně popisu jednotlivých polí/atributů události
    - Způsob uložení zalogovaných událostí
        - Jak jsou události uloženy
        - Kde
            - soubor (včetně cesty k souboru)
            - databáze, včetně:
                - DB serveru a názvu tabulky, případně tabulek
                - SQL dotazu pro sestavení view v případě, že událost je uložena do více tabulek
            - vzdálený server (IP adresa, protokol)
        - Jak dlouho jsou uloženy
        - Jak lze konfigurovat
    - Protokol logování (např. syslog, windows event log, W3C, apod.)
- Popis provozního monitoringu (např. SNMP, síťový monitoring, aplikační monitoring)
    - Popsat, jakým způsobem je realizován provozní monitoring za účelem identifikace a detekce požadovaných či nestandardních provozních stavů systému

Základní uživatelská příručka

Cíl dokumentu: vytvořit základní návod pro ovládání uživatelského rozhraní systému pro běžného uživatele. Zjednodušit běžnému uživateli základní orientaci v uživatelském rozhraní systému.

- Forma dokumentu: textový popis, textový popis doplněný o obrázky
- Popis provedení základních/běžných/rutinních funkcí, kroků a postupů, které uživatel může provádět

Základní administrátorská příručka

Cíl dokumentu: vytvořit základní návod pro ovládání administračního rozhraní systému pro administrátora. Zjednodušit privilegovanému uživateli základní orientaci v administračním rozhraní systému.

- Forma dokumentu: textový popis, textový popis doplněný o obrázky
- Popis provedení standardních (základních/běžných/rutinních) operací, které vedou k běžné administraci systému
- Popis provedení nestandardních (málo běžných) operací, pokud je třeba

Popis klíčových komponent

Cíl dokumentu: popsat a zdokumentovat účel, význam, úlohu a způsob použití klíčových komponent systému

- Forma dokumentu: textový popis (může být doplněno i o schéma)
- Základní fungování, účel, úloha jednotlivých klíčových komponent + jakou platformou (softwarem) jsou jednotlivé komponenty zajištěny
    - Např. master (server), agent (klient), různé typy použitých serverů, moduly, zdroje informací, příjemci informací (systémy), apod.

Příloha č. 3 - Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv objednatele

- Bezpečnost přístupových oprávnění
  - Poskytovatel je povinen chránit veškeré přístupové údaje k informačním aktivům objednatele včetně přístupů k informačním aktivům poskytovatele, které umožňují přístup k informačním aktivům objednatele či umožnují jejich správu.
  - Poskytovatel je povinen dodržovat tuto bezpečnostní politiku hesel pro výše uvedené přístupové údaje:
    - min. délka hesla 17 znaků
    - složitost hesla musí splňovat minimálně 3 ze 4 kategorií
      - malá písmena
      - velká písmena
      - číslice
      - speciální znaky
    - hesla musí být uchovávána v tajnosti, nesmí být ukládána v nezašifrované podobě (dle bodu kryptografie)
    - hesla nesmí obsahovat žádné informace z přihlašovacího jména (login)
    - platnost hesla musí být maximálně 1,5 roku.
  - Poskytovatel je povinen používat personifikované účty, které jsou nepřenosné na jiné osoby, než kterým byly údaje přiděleny.
  - Přístupová oprávnění lze využívat pouze pro ten účel, pro který byla zřízena.
  - Pokud by Poskytovatel zřizoval přístupová oprávnění třetí straně, je Poskytovatel povinen o této skutečnosti informovat objednatele. Objednatel má v tomto případě právo zřízení přístupu zamítnout.
- Řízení změn
  - Poskytovatel se zavazuje zaznamenávat všechny změny, které v informačním aktivu provedl.
  - Poskytovatel se zavazuje vynucovat zaznamenávání změn i u případných poddodavatelů.
  - Záznam změny musí obsahovat minimálně tyto informace:
    - Datum a čas změny
    - Jméno osoby, která změnu provedla
    - Název, popis a účel změny
- Objednatel si vyhrazuje právo na pravidelné informace o záznamech všech změn provedených dodavatelem i případnými poddodavateli.
  - Poskytovatel se zavazuje všechny změny jím provedené, změny případných poddodavatelů, poskytnout objednateli formou provozního deníku.
- Řízení rizik
  - Objednatel si vyhrazuje právo na informace o tom, jakým způsobem dodavatel řídí rizika v souvislosti s plněním této smlouvy, tedy o tom, jakou metodiku pro řízení rizik používá, jakým způsobem jsou rizika hodnocena a klasifikována, jakým způsobem jsou rizika ošetřována a kdo je za řízení rizik za dodavatele zodpovědný.
- Řízení kybernetických bezpečnostních incidentů:
  - Poskytovatel je povinen na KrÚ hlásit veškeré kybernetické bezpečnostní incidenty, které se týkají informačních aktiv objednatele nebo informačních

aktiv poskytovatele, pokud se kybernetický bezpečnostní incident týká informací či informačních aktiv poskytovatele.
    - Dodavatel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy Kraje Vysočina.
- Kryptografie:

Obecně

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

Hashovací funkce

Ukládání otisků hesel

- pro ukládání hesel uživatelů mohou být použity pouze tyto tzv. pomalé hashovací funkce:
    - Argon2i
    - bcrypt
    - scrypt
    - PBKDF2
- 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.

Elektronické podepisování e-mailů a dokumentů

- SHA-2 a vyšší
- délka otisku 256 bitů a vyšší

Ověřování integrity souborů

- SHA-2 a vyšší
- délka otisku 224 bitů a vyšší

Asymetrická kryptografie

SSL/TLS

- 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) - 2048 bitů a více (postupně přecházet na 3072 bitů, tam kde to bude možné)
            - 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 - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
            - 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
    - Způsob naplnění:
        - Diffie-Hellman implementace: https://weakdh.org/sysadmin.html
- Certifikáty dodá zadavatel

Šifrování, podepisování a autentizace

- týká se různých technologií PKI, PGP, S/MIME, SSH, apod.
- minimální délka klíče
    - algoritmus DSA – 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
    - algoritmus RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
    - algoritmus ECDSA - 256 bitů
- Ověřování (např. SSH klíče)
    - délka klíče minimálně 2048 bitů u RSA a DSA algoritmů (postupně přecházet na 3072 bitů, tam kde to bude možné)
    - délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky

Symetrická kryptografie

- nesmí být použity tyto šifry:
    - DES, 3DES, RC4, Blowfish, Kasumi
- minimální délka šifrovacího klíče - 128 bitů
    - pro šifru Chacha20 minimálně 256 bitů a se zatížením klíče menším než 256 GB
- nesmí být použity tyto módy pro ochranu integrity:
    - HMAC-SHA1, CBC-MAC-X9.19