**SMLOUVA**

O PROVOZU APLIKACE Meteoapp

č. objednatele:

uzavřená na základě ust. § 2586 a násl. a § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“)

Smluvní strany

**Objednatel:**  **Zlínský kraj**

Adresa: třída Tomáše Bati 21, 761 90 Zlín

IČO: 70891320

DIČ: CZ70891320

Zastoupený: Ing. Radimem Holišem, hejtmanem

a

**Zhotovitel:**  Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky

Adresa sídla: Nad Stráněmi 4511, 76001 Zlín

IČO: 70883521

DIČ: CZ70883521

Zřízena zákonem č. 404/2000 Sb., o zřízení Univerzity Tomáše Bati ve Zlíně

Zastoupená: doc. Mgr. Milanem Adámkem, Ph.D., děkanem

Článek I.

Předmětsmlouvy

1. Zhotovitel se touto smlouvou zavazuje **provést** na svůj náklad a pro **objednatele provoz Meteo aplikace** a všech jejích komponent (dále jen „Aplikace“) a objednatel se touto smlouvou zavazuje zajistit zhotoviteli součinnost při zajištění provozu, to vše za podmínek v této smlouvě dále uvedených.
2. Podmínky a požadavky na zajištění provozu Aplikace jsou uvedeny **v Příloze č. 1,** která je nedílnou součástí této smlouvy.
3. Aplikace je výsledkem projektu výzkumu, vývoje a inovací s názvem „Systém zpřesněné předpovědi konvektivních srážek pro krajský územní celek“ (VI20192022134) a jde o etapu implementace softwarové aplikace do praxe pracovníky krizového řízení objednatele.

Článek II.

Způsob, doba a místo plnění

1. Zhotovitel zajistí provoz Aplikace dle Přílohy č. 1 od 1. 4. 2022 do 31. 1. 2027.
2. Aplikace bude instalována v souladu s Přílohou č. 1 na serveru, který je umístěn v Technologickém centru Zlínského kraje (třída Tomáše Bati 21, 761 90 Zlín).

Článek III.

Spolupůsobení objednatele

1. Objednatel se zavazuje poskytnout nebo zprostředkovat zhotoviteli informace a prostředky nezbytné pro řádné plnění této smlouvy.
2. Objednatel se zavazuje poskytnout zhotoviteli veškerou součinnost potřebnou pro řádné plnění této smlouvy, kterou je možné po něm spravedlivě požadovat.

Článek IV.

Licenční podmínky a ochrana citlivých informací a práva průmyslového vlastnictví

1. Zhotovitel poskytuje v rámci plnění předmětu smlouvy objednateli licenci k oprávněnému užití Aplikace, v souladu s ustanovením § 2358 a následující občanského zákoníku, a to do 31. 1. 2027.
2. Objednatel se zavazuje, že neposkytne Aplikaci ani její části třetí osobě bez písemného souhlasu zhotovitele.
3. Veškeré informace technického, organizačního, příp. finančního charakteru, které si smluvní strany navzájem poskytnou v souvislosti s realizací této smlouvy a které budou

a) některou ze smluvních stran výslovně označeny za důvěrné,

b) splňovat definici důvěrné informace ve smyslu ustanovení § 1730 občanského zákoníku, nebo

c) tvořit předmět obchodního tajemství podle § 504 občanského zákoníku,

(dále jen „citlivé informace“), jsou smluvní strany oprávněny použít výhradně k plnění svých povinností z této smlouvy.

1. Citlivé informace jsou smluvní strany povinny chránit před jejich zneužitím třetími osobami. Smluvní strany se proto zejména zavazují nezpřístupnit citlivé informace třetím osobám bez předchozího výslovného písemného souhlasu dotčené smluvní strany. Smluvní strany mohou citlivé informace bez souhlasu dotčených smluvních stran sdělovat pouze svým zaměstnancům, kteří se podílejí na plnění této smlouvy, a to v míře nezbytné k naplnění účelu této smlouvy; ale i v takovém případě smluvní strany odpovídají za dodržení povinností sjednaných v tomto článku. Smluvní strany jsou povinny vhodnými právními nástroji zajistit, aby jejich zaměstnanci sjednaná opatření k ochraně citlivých informací podle této smlouvy dodržovali.
2. Povinnost chránit citlivé informace podle odstavce 3 trvá i po skončení doby platnosti této smlouvy, a to bez ohledu na to, z jakých důvodů k němu dojde, nejdéle však do doby, kdy se předmětné citlivé informace stanou obecně známými nebo kdy ztratí charakter obchodního tajemství z rozhodnutí jejich vlastníka nebo jinak než porušením této smlouvy.
3. Za porušení povinností stanovených v odstavcích 3 a 4 se nepovažuje situace, kdy je smluvní strana povinna zpřístupnit citlivé informace osobám k tomu oprávněným na základě příslušného právního předpisu.

Článek V.

Cena a platební podmínky

1. Aplikace „MeteoApp“ bude provozována na hardwarových prostředcích objednatele bezplatně.
2. Zhotovitel provozuje aplikaci na hardwarových prostředcích objednatele bezplatně a neúčtuje objednateli žádné další poplatky (např. odměnu za licenci), stejně tak náklady na elektřinu, chlazení a na technickou podporu.

Článek VI.

Sankce a náhrada škody

1. Strany nejsou oprávněny požadovat žádnou smluvní pokutu.
2. Zhotovitel je odpovědný objednateli za plnění povinností vyplývajících z této smlouvy a za škodu způsobenou mu v souvislosti s plněním předmětu této smlouvy, a to i tehdy, byla-li škoda v této souvislosti způsobena zástupcem či pracovníkem zhotovitele nebo jeho poddodavatelem. V případě vzniku škody definované v tomto odstavci se zavazuje její výši zhotovitel objednateli uhradit, pakliže objednatel vůči zhotoviteli právo na náhradu škody uplatní.
3. V případě, že objednatel poruší své povinnosti vyplývající z této smlouvy a způsobí tím škodu nebo jinou újmu na straně zhotovitele, zavazuje se uhradit její výši zhotoviteli, pakliže zhotovitel vůči objednateli právo na náhradu škody uplatní.

Článek VII.

Odstoupení od smlouvy

1. Případná práva a povinnosti smluvních stran z odstoupení od smlouvy budou řešena podle příslušných ustanovení občanského zákoníku.
2. Za podstatné porušení smlouvy zhotovitelem se považuje podstatné porušení povinností ve smyslu ust. § 2002 odst. 1 občanského zákoníku a dále to, když:
* zhotovitel i přes písemnou výtku objednatele provozuje Aplikaci způsobem, který vede nepochybně k vadnému plnění,
* zhotovitel nebo jeho zaměstnanci poruší pravidla bezpečnosti pro práci v informačním systému uvedená v příloze č. 2 této smlouvy, konkrétně v jejím článku 1 odstavci c), d), e), f), h), článku 2 odstavci a), článku 3 odstavci b), d), článku 4 odstavci e), f), g), článku 5 odstavci a), d), e), f), g), článku 6 odstavci d), článku 7 odstavci a), b), článku 8 odstavci a), článku 9 odstavci b) a článku 10 odstavci a), b) c).

Článek VIII.

Organizace a komunikace

1. V průběhu plnění smlouvy se smluvní strany setkávají v sídle objednatele (nedohodnou-li se kontaktní osoby / zástupci jinak), aby konzultovali průběh plnění. Podrobnosti organizace a komunikace dohodnou smluvní strany na svém prvním jednání ve formě písemného zápisu podepsaného všemi zúčastněnými osobami. Jednání organizuje zhotovitel, který připravuje podklady pro jednání, vyhotovuje zápisy z jednání, prezenční listiny apod. Veškeré zápisy a listiny vzešlé z jednání obdrží obě smluvní strany. Zhotovitel bude při plnění této smlouvy postupovat dle zásad projektového řízení. Ze všech jednání mezi smluvními stranami budou vyhotoveny zápisy. Zápisy vyhotovuje zhotovitel již v průběhu jednání, po jednání je objednatel připomínkuje a obě smluvní strany je odsouhlasí podpisem. Všechny dokumenty, které bude zhotovitel zpracovávat, bude objednateli předávat k připomínkování průběžně.
2. Kontaktní údaje smluvních stran

Univerzita Tomáše Bati ve Zlíně – Ing. David Šaur, Ph.D.

Zlínský kraj - Ing. Robert Olša.

Adresa do systému Helpdesk pro hlášení vad a reklamací je uvedena v příloze č. 1 této smlouvy, kde kontaktní osobou bude Ing. Robert Olša.

Pokud zástupci – kontaktní osoby ve věcech technických uvedených v příloze č. 1 nedosáhnou shody ohledně řešení problému při plnění této smlouvy, postoupí se problém k řešení zástupcům – kontaktním osobám ve věcech smluvních. Pokud ani zástupci – kontaktní osoby ve věcech smluvních (za objednatele Ing. Robert Olša, za zhotovitele Ing. David Šaur, Ph.D.) nedosáhnou shody ohledně řešení takového problému, postoupí se problém k řešení na úroveň vyššího managementu smluvních stran.

1. Pokud dojde ke změně v údajích uvedených v odstavci 2 tohoto článku, jsou smluvní strany povinny změnu písemně oznámit druhé smluvní straně, a to předem nebo bezodkladně poté, co ke změně dojde. Za dostačující formu oznámení změny je považováno zaslání e-mailu kontaktní osobě druhé smluvní strany ve věcech smluvních, která je povinna obdržení e-mailu do 2 pracovních dnů potvrdit. V případě změny v kontaktních údajích uvedených v tomto odstavci není třeba uzavírat dodatek ke smlouvě.
2. Nastanou-li u některé ze smluvních stran skutečnosti bránící řádnému plnění této smlouvy, je povinna to ihned bez zbytečného odkladu oznámit druhé straně.

Článek IX.

Ochrana informací a závazek mlčenlivosti

1. Důvěrnými informacemi se pro účely této smlouvy a po celou dobu trvání vzájemné spolupráce Smluvních stran rozumí, bez ohledu na formu a způsob jejich sdělení či zachycení a až do doby jejich zveřejnění, jakékoli a všechny skutečnosti, které se Zhotovitel v průběhu vzájemné spolupráce dozví, a/nebo které mu Objednatel v průběhu vzájemné spolupráce zpřístupní (dále jen „důvěrné informace“), které jsou za důvěrné označeny.
2. Důvěrné informace touto smlouvou chráněné tvoří rovněž veškeré skutečnosti technické, ekonomické, právní a výrobní povahy v hmotné nebo nehmotné formě, které byly Objednatelem takto označeny a byly poskytnuty Zhotoviteli. Důvěrné informace mohou být dále společně označeny též jako „chráněné informace“.
3. Zhotovitel je povinen zajistit utajení získaných důvěrných informací způsobem obvyklým pro utajování takových informací, není-li výslovně sjednáno jinak. Tato povinnost platí bez ohledu na ukončení účinnosti této smlouvy. Objednatel má právo požadovat doložení dostatečnosti utajení důvěrných informací. Zhotovitel je povinen zajistit utajení důvěrných informací i u svých zaměstnanců, zástupců, jakož i jiných spolupracujících třetích stran, pokud jim takové informace byly poskytnuty.
4. Právo užívat, poskytovat a zpřístupnit důvěrné informace má Zhotovitel pouze v rozsahu a za podmínek nezbytných pro řádné plnění práva a povinností vyplývajících z této smlouvy.
5. Za důvěrné informace se podle této smlouvy bez ohledu na formu jejich získání považují veškeré informace, které se týkají obsahu, struktury a zabezpečení informačních systémů Objednatele.
6. Za důvěrné informace se v žádném případě nepovažují informace, které se staly veřejně přístupnými, pokud se tak nestalo porušením povinnosti jejich ochrany, dále informace získané na základě postupu nezávislého na této smlouvě nebo Objednatelem, pokud je Zhotovitel schopen tuto skutečnost doložit, a konečně informace poskytnuté třetí osobou, která takové informace nezískala porušením povinnosti jejich ochrany.
7. Zhotovitel se zavazuje zavázat k mlčenlivosti i veškeré své zaměstnance, jakož i veškeré třetí osoby, které by mohly přijít s takovými informacemi v rámci své činnosti, byť nahodile, do styku.
8. Závazky k zachovávání důvěrnosti informací zůstanou v plném rozsahu platné a účinné i po ukončení platnosti a účinnosti této smlouvy, a to až do doby, kdy se tyto stanou obecně známými jinak než porušením této smlouvy, nebo je Objednatel přestane utajovat; v pochybnostech se má za to, že utajování informací trvá.
9. Po ukončení účinnosti této smlouvy je Zhotovitel povinen bez zbytečného odkladu vrátit Objednateli všechny poskytnuté materiály obsahující důvěrné informace včetně jejich případně pořízených kopií. O předání a převzetí se sepíše protokol podepsaný oběma smluvními stranami.

Článek X.

Bezpečnostní pravidla

1. Zhotovitel se zavazuje dodržovat Pravidla bezpečnosti pro práci v informačním systému uvedená v Příloze č. 2. této smlouvy.
2. Zhotovitel se zavazuje, že jeho zaměstnanci budou při svých činnostech dodržovat a zachovávat bezpečnostní pravidla uvedena v Příloze č. 2. této smlouvy.
3. Zhotovitel se zavazuje, že seznámí všechny své zaměstnance, kteří budou do informačních systémů nebo do prostor objednatele přistupovat, s bezpečnostními pravidly před začátkem jakýchkoliv aktivit.
4. Přihlašovací údaje do informačních systémů nebo přístupů do prostor objednatele budou předávány na základě jednotlivých písemných protokolů, z nichž každá smluvní strana obdrží po jednom výtisku.

Článek XI.

Zpracování a ochrana osobních údajů

1. Tento článek smlouvy upravuje vzájemná práva a povinnosti smluvních stran při zpracování osobních údajů, ke kterému dochází v souvislosti s plněním předmětu této smlouvy. Smluvní strany jsou v souvislosti s ochranou osobních údajů povinny dostát všem povinnostem, které vyplývají z právních předpisů platných a účinných na území České republiky (dále jen „ČR“).
2. Pro účely tohoto článku se za správce osobních údajů považuje Univerzita Tomáše Bati ve Zlíně (dále také jako „správce“), která zajišťuje provoz Meteo aplikace a všech jejích komponent pro objednatele. Za zpracovatele se považuje Zlínský kraj (dále také jako „zpracovatel“), který monitoruje a eviduje aktivity zaměstnanců správce při přístupu do segmentu krizového řízení a činnosti při zpracování dat a v této souvislosti zpracovává osobní údaje subjektu údajů. Zpracovatel je povinen ve vztahu k osobním údajům, které zpracovává, dodržovat stejné zásady a povinnosti jako správce.
3. Smluvní strany prohlašují, že jsou zpracovávány tyto osobní údaje:
4. příjmení,
5. jméno, popřípadě jména.

Zpracování osobních údajů bude prováděno zejména shromážděním, uložením.

1. Smluvní strany prohlašují, že jsou schopny zajistit technické a organizační zabezpečení ochrany osobních údajů. V této souvislosti se smluvní strany zavazují zejména přijmout veškerá opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, jakož i jejich zneužití, a dále také opatření týkající se práce s příslušnými informačními systémy, vymezením omezeného okruhu osob, jež mohou disponovat s osobními údaji, včetně zajištění jejich mlčenlivosti o údajích, které se v rámci zpracování osobních údajů dozvědí, zajištění místností a počítačů s databázemi proti vniknutí třetích osob, tj. bezpečnostní zámky, hesla do počítačů, antivirové programy, bezpečnostní zálohy a další vhodné nástroje. V případě jakéhokoliv porušení zabezpečení osobních údajů je zpracovatel povinen v souladu s příslušnými právními předpisy zaslat správci bez zbytečného odkladu informace o takovém narušení. Informace o takovém porušení musí obsahovat:
2. popis povahy porušení zabezpečení osobních údajů, kategorií a přibližný počet dotčených subjektů údajů a kategorií a přibližný počet dotčených záznamů osobních údajů,
3. jméno a kontaktní údaje na pověřence pro ochranu osobních údajů, pokud byl jmenován,
4. popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
5. popis opatření, které zpracovatel přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů včetně případných opatření ke zmírnění možných nepříznivých dopadů.
6. Správce a zpracovatel se dále zavazují:
7. nezneužívat osobní údaje k jinému než stanovenému účelu podle této smlouvy,
8. učinit s odbornou péčí všechna kontrolní a ochranná opatření za účelem ochrany osobních údajů,
9. s odbornou péčí dodržovat všechna kontrolní a ochranná opatření za účelem ochrany osobních údajů,
10. neprodleně reagovat na žádosti subjektů údajů, tyto informovat o všech jejich právech a na žádost umožnit přístup k informacím o zpracování, opravu osobních údajů, blokování, doplnění a veškeré takové požadavky se smluvní strany zavazují vzájemně si předávat; zpracovatel se zavazuje informovat správce o všech skutečnostech majících vliv na zpracování osobních údajů,
11. oznámit každou pochybnost o dodržování příslušných právních předpisů platných a účinných na území ČR či narušení bezpečnosti osobních údajů,
12. bude-li to třeba, poskytnout si vzájemně veškerou součinnost při styku a jednáních s Úřadem pro ochranu osobních údajů a se subjekty údajů,
13. dodržovat všechny ostatní povinnosti stanovené příslušnými právní předpisy platnými a účinnými na území ČR, i pokud tak není výslovně uvedeno v této smlouvě,
14. vynaložit veškeré možné úsilí na odstranění protiprávního stavu ve vztahu k osobním údajům dle této smlouvy, kterým by došlo k porušení povinností stanovených příslušnými právními předpisy platnými a účinnými na území ČR jednáním příslušné smluvní strany, a to neprodleně poté, co taková skutečnost nastane,
15. přijmout opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce.
16. Zpracovatel se zavazuje, že nezapojí do zpracování žádného dalšího zpracovatele.
17. Osobní údaje budou zpracovávány pouze po dobu účinnosti a platnosti této smlouvy. Po uplynutí této doby budou osobní údaje bezodkladně vráceny správci nebo prokazatelně na základě písemného požadavku správce zlikvidovány. Zpracovatel je povinen nejpozději do 10 dnů po doručení takového požadavku osobní údaje zlikvidovat. Pokud existují kopie zpracovávaných osobních údajů, je zpracovatel povinen je vymazat.
18. Správce je kdykoliv oprávněn kontrolovat plnění a dodržování kteréhokoliv ustanovení tohoto článku, a to i bez předchozího upozornění, a smluvní partner je povinen takovou kontrolu správci umožnit a poskytnout mu veškeré informace potřebné k doložení toho, že jsou splněny veškeré povinnosti vyplývající z tohoto článku.
19. V případě, že zpracovatel poruší své povinnosti uvedené v tomto článku a své porušení neodstraní ani po předchozím písemném upozornění správce v přiměřené lhůtě k tomu mu správcem poskytnuté, je správce oprávněna od této smlouvy odstoupit.
20. V případě, že v důsledku porušení povinností na straně zpracovatele vznikne správci škoda, je zpracovatel povinen tuto škodu správci uhradit, a to na základě výzvy správce adresované zpracovateli.
21. Zpracovatel není oprávněn osobní údaje jakkoliv nad rámec této smlouvy nebo v rozporu s ní dále zpracovávat, zapojit do zpracování dalšího zpracovatele nebo osobní údaje předávat a převádět třetím osobám či jiným zpracovatelům, pokud správce písemně neurčí jinak. Pokud zpracovatel zpracovává osobní údaje v rozporu s touto smlouvou nebo nad její rámec platí, že osobní údaje nezpracovává pro účely a v rozsahu pro správce a správce za to nenese žádnou odpovědnost. Ve vztahu k osobním údajům takto zpracovávaným je zpracovatel v postavení správce s veškerou odpovědností z toho vyplývající.

Článek XII.

Audit

1. Zhotovitel umožní Objednateli či třetím osobám zvoleným Objednatelem přístup do prostor Zhotovitele za účelem kontroly, zda plnění bezpečnostních pravidel dle článku X. je poskytováno v souladu s touto smlouvou (dále jen „Audit“).
2. Zhotovitel je v souvislosti s Auditem povinen poskytnout Objednateli veškerou nezbytnou součinnost.
3. Pokud Audit prokáže, že Zhotovitel nesplnil své povinnosti vyplývající z této smlouvy, uplatní se ustanovení článku VI. této smlouvy.

Článek XIII.

Závěrečná ujednání

1. Smlouva podléhá zveřejnění v Registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Smluvní strany se dohodly, že objednatel v zákonné lhůtě odešle tuto smlouvu k řádnému uveřejnění do registru smluv vedeného Ministerstvem vnitra ČR. O uveřejnění této smlouvy objednatel bezodkladně informuje zhotovitele (postačí e-mailem prostřednictvím kontaktní osoby/zástupce ve věcech technických nebo smluvních). V případě, že ihned po podpisu této smlouvy není jednou ze smluvních stran oznámeno písemně druhé smluvní straně (postačí e-mailem prostřednictvím kontaktní osoby/zástupcem ve věcech technických nebo smluvních), že smlouva nebo její přílohy obsahují obchodní tajemství, má se za to, že tato smlouva nebo její přílohy neobsahují obchodní tajemství.
2. Tuto smlouvu lze změnit nebo doplňovat pouze písemnými dodatky, které budou podepsány oběma smluvními stranami, není-li v ní uvedeno jinak.
3. Nedílnými součástmi této smlouvy jsou následující přílohy:
4. Příloha č. 1: Specifikace Aplikace
5. Příloha č. 2: Pravidla bezpečnosti pro práci v informačním systému.

Pokud se v těchto přílohách hovoří o zadavateli, myslí se jím objednatel. Pokud se v těchto přílohách hovoří o dodavateli, uchazeči, účastníkovi nebo poskytovateli, myslí se jím zhotovitel. Pokud je v těchto přílohách něco upraveno odlišně než v textu smlouvy samotné, přednost má text smlouvy samotné.

1. V souladu s ustanovením § 1801 občanského zákoníku se ve smluvním vztahu založeném touto smlouvou vylučuje použití ustanovení § 1799 a § 1800 občanského zákoníku.
2. Práva a povinnosti smluvních stran výslovně v této smlouvě neupravená se řídí příslušnými ustanoveními občanského zákoníku.
3. Případná neplatnost některého ustanovení této smlouvy nemá za následek neplatnost ostatních ustanovení. V případě, že kterékoliv ustanovení této smlouvy se stane neúčinným nebo neplatným, smluvní strany se zavazují bez zbytečného odkladu nahradit takové ustanovení novým, které svým obsahem a smyslem odpovídá nejlépe obsahu a smyslu ustanovení původního.
4. Smluvní strany této smlouvy prohlašují a stvrzují svými podpisy, že mají plnou způsobilost k právním úkonům, a že tuto smlouvu uzavírají svobodně a vážně, že ji neuzavírají v tísni, ani za jinak nápadně nevýhodných podmínek, že si ji řádně přečetly a jsou srozuměny s jejím obsahem.
5. Tato smlouva se vyhotovuje ve 3 stejnopisech s platností originálu, z nichž 2 obdrží objednatel a 1 zhotovitel.
6. Smlouva nabývá platnosti dnem, kdy byla podepsána oběma stranami, a účinnosti tím dnem, kdy bude uveřejněna prostřednictvím registru smluv. Uveřejnění v registru smluv zabezpečí zhotovitel neprodleně po podpisu smlouvy oběma smluvními stranami.
7. Smluvní strany se dále dohodly, že tato smlouva a její ustanovení ode dne nabití její účinnosti plně nahrazuje veškeré předchozí ústní či písemné smlouvy a ujednání mezi smluvními stranami týkající se předmětu této smlouvy.

**Doložka dle § 23 zákona č. 129/2000 Sb., o krajích, ve znění pozdějších předpisů**

Schváleno orgánem kraje: RZK

Datum jednání a číslo usnesení: 14. 3. 2022, 0213/R08/22

Ve Zlíně dne:Ve Zlíně dne:

za objednatele: za zhotovitele:

…………………………….…. …………………………………

Ing. Radim Holiš doc. Mgr. Milan Adámek, Ph.D.

Zlínský kraj děkan UTB FAI

hejtman

**Příloha č. 1: Specifikace aplikace**

Specifikace Aplikace

Aplikace Meteo slouží k předpovědi přívalových povodní a dalších meteorologických jevů a včasnému varování využívané hlavně krizovým řízení kraje

Aplikace nebude veřejně přístupná, pouze v rámci krizového řízení, tzn. ve fyzicky oddělené síti IVVS. Aplikace nevyužívá žádné uživatelské profily či role, uživatelé nejsou autentizováni pro přístup do Aplikace. Aplikace ale bude obsahovat více aplikačních administrátorských účtů pro technické správce. Techničtí správci Zhotovitele budou mít zajištěn přístup na server pomocí VPN technologie Objednatele. Z pohledu zálohování bude aplikační server zálohován standardním způsobem jako ostatní servery provozované objednatelem. Aktualizace systému probíhají v rámci operačního systému a budou nastaveny zhotovitelem v rámci implementace (systém automatických aktualizací prostřednictvím Windows Update služby, pokud objednatel nerozhodne jinak). Zhotovitel se zavazuje k zajištění implementace bezpečnostních záplat Aplikace a OS nejpozději do 14 dnů od jejich vydání.

Aplikace nepřetěžuje hardwarové prostředky neobvyklým způsobem (výjimkou mohou být předem naplánované úlohy typu dávkové zpracování dat).

**Aplikaci Meteo bude splňovat**

* + - 1. Součástí dodávky bude i zaškolení uživatelů a administrátorů Aplikace min. v rozsahu 2hod.
			2. V době předání bude mít Aplikace nainstalovány všechny relevantní bezpečnostní záplaty a stanoveny mechanismy pro implementaci aktuálních bezpečnostních záplat během provozu.
			3. Zhotovitel se zavazuje, že na Aplikaci provedl v rámci vývoje úspěšné penetrační testy. Během provozu Aplikace na Krajském úřadě Zlínského kraje (dále jen „KÚZK“) a tohoto smluvního vztahu objednatele a zhotovitele zajišťuje zhotovitel Aplikace pravidelné penetrační testování minimálně jednou za rok. Aplikace bude testována minimálně na zranitelnosti definované v OWASP Top 10. Zhotovitel vyhotovuje záznamy o penetračním testování a výsledky předloží na požádání.
			4. Aplikace musí být chráněna proti bezpečnostním chybám, u webových řešení je vyžadováno splnění doporučení **aktuálního** OWASP Top 10 pro rok 2021 ([https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project](https://www.owasp.org/index.php/Category%3AOWASP_Top_Ten_Project)), které popisuje 10 nejčastějších zranitelností např.
	+ Broken Access Control
	+ Injection (zejména SQL, NoSQL, OS a LDAP injection, technika napadení vrstvy programu vsunutím kódu přes neošetřený vstup a vykonání vlastního dotazu) atd.
	+ Identification and Authentication Failures (často nekorektně implementovaná autentizace a správa session dovolující útočníkům kompromitaci hesel, session tokenů atd.).
		- 1. Aplikace musí přistupovat do databáze jen prostřednictvím jednoho speciálního „společného“ účtu. (Není možno pro přístup do databáze používat účty uživatelů.) Tento účet musí být odlišný od administrátorského účtu, který bude používán pro správu / vzdálenou správu.
			2. Zajištění logování Aplikace dle 2. odst. §22 vyhlášky 82/2018 Sb., např. informace o činnosti uživatelů a administrátorů (přihlášení, odhlášení, manipulace s účty a oprávněními, úspěšné i neúspěšné pokusy činností, kritické i chybové hlášení apod.).
			3. Ovládání Aplikace bude v českém jazyce.
			4. Součástí dodávky Aplikace musí být všechny dodávané licence a licenční ujednání, včetně licencí a licenčních ujednání podpůrných nástrojů, které jsou součástí dodávky.
			5. Objednatel s ohledem na předpokládaný dlouhodobý provoz a životnost pořizovaného řešení požaduje, aby byla Aplikace postavena na současných, a nikoliv již překonaných/opouštěných technologiích, které zajistí dlouhodobou podporu daného řešení. Za překonané/opouštěné technologie jsou objednatelem považovány takové, u kterých v příštích 2 letech jejich tvůrce ukončí podporu jejich životního cyklu a dále takové, jejichž vývoj a podpora již byly ukončeny.
			6. Aplikace musí splňovat všechny zákonné normy a standardy. Pro webovou část se jimi rozumí zvláště:
				1. zákon 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 (WCAG 2.1)
				2. HTML 5, CSS 3
				3. metodika Bliend Ffrienly Web 2.3 (<http://blindfriendly.cz/metodiky>).
			7. Webová Aplikace musí být optimalizována pro běžně používané internetové desktopové prohlížeče. Podporovaná je vždy aktuální a jedna předchozí verze poslední vydané číselné řady prohlížeče: Microsoft Edge, Mozilla Firefox, Opera, Google Chrome, Safari.
			8. Aplikace musí být optimalizována, aby z hlediska výkonnosti byly při práci uživatelsky přívětivé doby odezev. Webová Aplikace musí mít:
				1. Správně strukturovaný HTML kód.
				2. Komprimace a minifikace vkládaných skriptů (aby se zbytečně nenačítaly desítky CSS a JS souborů).
				3. Musí mít použity optimalizované obrázky v co nejmenších velikostech

komprimace např. TinyPNG, TinyJPG;

co nejvíce omezený počet bitmap s důrazem na větší využití vektorů (SVG, pro piktogramy vytvořit např. font atd.)

* + - * 1. První request (first byte) vyřízený do 300ms
				2. Maximální doba odezvy Aplikace pro 30 konkurenčních uživatelů bude 2 sekundy na poskytnutých HW prostředcích KÚZK specifikovaných níže, garance této doby je pro uživatele přistupující ze sítě IVVS.
			1. Součástí dodávky Aplikace bude kompletní „Provozní dokumentace“, obsahem bude zejména:

- Bezpečnostní dokumentace informačního systému veřejné správy - popis realizovaných bezpečnostních opatření, mechanismů a jejich návazností,

- Systémová příručka,

- Uživatelská příručka,

Dokumentace bude také obsahovat podrobný popis implementace. Tento popis bude součástí Systémové příručky nebo může být uveden v samostatném dokumentu. Veškerá dokumentace bude předána v elektronické podobě v českém jazyce.

Členění obsahu jednotlivých částí dokumentace:

1. **Implementační část** – vznikne společnými silami zhotovitele a Implementačního týmu, bude v ní popsáno co, na kterých serverech a kde je nainstalováno, nastaveno, jaké služby a úlohy v jaké časové intervaly a pod jakými účty jsou spouštěny. Stručný a věcný popis, minimálně vyznačené části v systémové a bezpečnostní části pomocí zkratky [impl]. Podrobnější popis pak bude uveden ve finální systémové a bezpečnostní části.
2. **Systémová část:**
	* schéma a popis aplikační a systémové architektury a infrastruktury – topologie, popis struktury adresářů a databáze atd. [impl]
	* systémové požadavky pro běh Aplikace, [impl]
	* nastavení proti přetěžování systému, [impl]
	* popis aplikačních rozhraní pro možnosti aplikační, popř. procesní integrace
	* popis existujících vazeb (např. napojené datové zdroje) [impl]
	* režim správy Aplikace (kdo, co spravuje) [impl]
	* princip aktualizace
	* seznam licencí
	* plány nasazování aktualizací, podle nichž budou průběžně vydávané záplaty testovány a následně aplikovány na IS
3. **Bezpečnostní část** - popis realizovaných bezpečnostních opatření, mechanismů a jejich návazností:
	* popis veškerých metod přístupů např.: aplikace přistupuje k DB – bude uveden účet a odkaz na umístění hesla, četnost (pokud jde o relevantní údaj) apod. [impl]
	* popis autorizace a autentizace uživatele [impl]
	* popis uživatelských rolí, jejich oprávnění [impl]
	* popis správy uživatelů [impl]
	* logování – kam se loguje, kde se nastavuje úroveň logování, co se loguje v návaznosti na bod 6)
	* zálohování - co, jak často, na jak dlouho, kam, jakým způsobem atd. [impl]
	* popis a návod k využívání bezpečnostních funkcí (pokud jsou implementovány), vztah k jednotlivým rolím, k činnosti správce (např. doba timeout session, SMS při určitých akcích, kdo může prohlížet logy, spouštět synchronizaci datových zdrojů apod.)
	* popis naplnění doporučení OWASP Top10, jedná-li se o webovou aplikaci.
4. **Provozní část**
	* administrátorská příručka
	* uživatelská příručka.

**Požadavky na HW vybavení**

8 CPU

24 GB RAM

200 GB SSD HDD

Konektivita do internetu a připojení k meteoradaru ZK (viz seznam zdrojů dat)

OS Windows Server 2016/2019

Microsoft SQL Server Express

**Schéma aplikace**

MeteoAlg

Internet

WebApp

Scheduler

DataStore

SQL

Integrační API

Meteoradar

**Datové zdroje**

|  |  |
| --- | --- |
| **Parametr** | **Zdroje:** |
| Oblačnost | https://www.chmi.cz/ |
| Relativní\_vlhkost\_1000 | https://www.chmi.cz/ |
| Srážky | https://www.chmi.cz/ |
| Mixing\_Ratio\_0-1km | http://www.lightningwizard.com/ |
| MUCAPE | http://www.lightningwizard.com/ |
| Teplota\_850 | http://www1.wetter3.de/ |
| MLCAPE+LI\_Wetter\_3\_de | http://www1.wetter3.de/ |
| MLCIN\_Wetter\_3\_de | http://www1.wetter3.de/ |
| Wet\_bulb\_temp | http://www1.wetter3.de/ |
| Frontogeneze\_parametr\_850\_hPa | http://www1.wetter3.de/ |
| Radarové\_snímky | [http://portal.chmi.cz/](http://portal.chmi.cz/files/portal/docs/meteo/rad/data_tr_png_1km/pacz23.z_max3d)  |
| Radary\_srážkoměry | http://hydro.chmi.cz/ |
| MFDIV\_0-1km | http://www.modellzentrale.de/ |
| Potential\_Orograpic\_Lift | http://www.modellzentrale.de/ |
| Pwater | http://www.modellzentrale.de/ |
| Relativni\_vorticita\_850-300\_hPa\_WRF | http://www.modellzentrale.de/ |
| Relativní\_vlhkost\_700 | http://www.modellzentrale.de/ |
| SRH\_3km\_WRF\_ARW | http://www.modellzentrale.de/ |
| Srážky\_MAIN | http://www.modellzentrale.de/ |
| Tlaková\_tendence\_MSLP | http://www.modellzentrale.de/ |
| Vítr\_300 | http://www.modellzentrale.de/ |
| Srážky\_MAIN | http://flymet.meteopress.cz/ |
| Vítr\_10m | http://flymet.meteopress.cz/ |
| Vítr\_500 | http://flymet.meteopress.cz/ |
| Vítr\_600 | http://flymet.meteopress.cz/ |
| Vítr\_700 | http://flymet.meteopress.cz/ |
| Vítr\_850 | http://flymet.meteopress.cz/ |
| Směry\_větru | https://www.windguru.cz/ |
| DLS | https://www.weatheronline.cz/ |
| LLS | https://www.weatheronline.cz/ |

Technické kontakty:

Ing. David Šaur, Ph.D., saur@utb.cz, tel: 731 948 537

Ing. Jaromír Švejda, Ph.D., svejda@utb.cz, tel: 732 203 582

Ing. Roman Žák, Ph.D, zak.roman4@gmail.com, tel: 723 414 609

Ing. Jakub Řeha, kbcz@famoz.cz, tel: 732 812 617

Mgr. Ladislav Gaál, ladislav.gaal@microstep-mis.com, 731 520 955

Ing. Robert Olša, robert.olsa@kr-zlinsky.cz, 731 555 143

Odpovědné osoby:

Ing. David Šaur, Ph.D., saur@utb.cz, tel: 731 948 537

Ing. Robert Olša, robert.olsa@kr-zlinsky.cz, 731 555 143

**Příloha č. 2**

**Bezpečnostní pravidla pro práci v informačním systému (IS)**

ICT (informační a komunikační technologie) jsou veškeré informační technologie používané pro komunikaci a práci s informacemi

IS (Informační systém) je celek složený z počítačového hardwaru, souvisejícího softwaru a dat.

1. **Přístup k IS ZK**
2. Přístup jiných subjektů (dále jen druhá smluvní strana) k IS ZK je možný pouze na základě smluvně ošetřeného vztahu se Zlínským krajem.
3. Druhá smluvní strana je povinna dodržovat bezpečnostní pravidla pro práci v IS ZK a nese v souladu s platnou legislativou a předpisy svůj díl odpovědnosti za nedodržení či porušení pravidel, případně za škody vzniklé v důsledku bezpečnostních incidentů, které zavinila.
4. Je přísně zakázáno vykonávat jiné než dohodnuté činnosti, přistupovat k jiným než povoleným prostředkům, serverům a datům. Dále je zakázáno provádět jakékoli úkony směřující k zjišťování rozsahu přidělených oprávnění, dostupnosti síťových prostředků a služeb a způsobů zabezpečení.
5. Druhá smluvní strana je povinna používat pouze jí přidělené přístupy a povolené způsoby přístupu, (fyzické přístupy, přístupové údaje, povolené časy pro přístup a přidělená oprávnění), a je odpovědná za jejich používání, za svou činnost v IS ZK a dodržování bezpečnostních pravidel při práci s informacemi. Přidělené údaje jsou pro druhou smluvní stranu závazné, jsou důvěrné a jsou platné jen po dobu platnosti smlouvy. Tyto údaje jsou uvedeny ve smlouvě nebo v Předávacím protokolu k účtu.
6. Přístupy a přístupová oprávnění jsou přidělena pouze v rozsahu nezbytně nutném pro výkon smluvních závazků. Druhá smluvní strana nesmí do přidělených oprávnění zasahovat a měnit je. Pokud zjistí, že oprávnění jsou odlišná od dohodnutých, neprodleně na to upozorní odpovědné osoby nebo Správce IS.
7. Druhá smluvní strana nesmí vytvářet žádné přístupové cesty do IS ZK a měnit přístupová oprávnění. Tyto změny může provádět Správce IS na základě písemné žádosti.
8. Přistupovat k IS ZK mohou pouze poučení pracovníci druhé smluvní strany. Druhá smluvní strana zajistí před zahájením prací poučení a proškolení všech svých pracovníků a poddodavatelů, kteří budou přistupovat k IS ZK.
9. Pracovníci druhé smluvní strany jsou povinni řídit se pokyny odpovědných osob (uvedených ve smlouvě), Správců IS a dalších pracovníků oddělení informatiky.
10. Činnost druhé smluvní strany v IS ZK je monitorována a evidována. Pověření pracovníci ZK mohou ověřovat dodržování stanovených bezpečnostních pravidel a zakázat neoprávněné aktivity.
11. Porušení bezpečnostních pravidel je sankcionováno vypovězením smlouvy.
12. Druhá smluvní strana je povinna předávat informace o provedených zásazích a změnách, a bez zbytečného prodlení je promítnout do dokumentace.
13. **Účty a hesla**
14. Přidělené přihlašovací účty jsou chráněny heslem. Názvy přihlašovacích účtů a hesla nesmějí být sděleny žádné neoprávněné osobě, pouze osobám dle bodu 1. písm. g). Heslo musí splňovat aktuální požadavky na kvalitu a platnost a musí být uchováno v tajnosti. Pokud je to možné, je použita vícefaktorová autentizace.
15. Mimo dohodnuté časy jsou přístupové účty neaktivní. V případě potřeby mohou jejich aktivaci schválit a zajistit odpovědné osoby.
16. Při porušení bezpečnostních pravidel druhou smluvní stranou mohou být přidělené přístupové účty zablokovány nebo zcela odebrány.
17. **Vzdálený přístup a vzdálená údržba**
18. Vzdálený přístup do IS ZK je možný pouze níže dohodnutým způsobem. Vzdálený přístup je vždy šifrován.
19. Přístup je možný pouze z pracovní stanice, která má nainstalovaný podporovaný operační systém, nainstalovány všechny bezpečnostní záplaty operačního systému vydané výrobcem, a má aktivní a aktuální antivirovou ochranu.
20. Pro zvýšení bezpečnosti může být vzdálený přístup umožněn pouze z ověřených konkrétních předem definovaných IP adres druhé smluvní strany.
21. Přístup k systémům v oblastech s vysokou úrovní zabezpečení za účelem vzdálené údržby (např. u významných informačních systémů ZK) musí být chráněn kromě šifrování i silnou autentizací druhé smluvní strany.
22. Pracovní stanice určené k přístupu do IS ZK ze vzdálené lokality musí být fyzicky zabezpečeny proti přístupu neoprávněných osob.
23. **Zabezpečení fyzického přístupu k IS**
24. Servery, síťové komponenty a další ICT zařízení jsou zabezpečeny proti fyzickému přístupu. Přístup do místností se servery s citlivými daty a přístup k síťovým zařízením je regulován a odpovídajícím způsobem monitorován. Pokud fyzické zabezpečení citlivých dat není dostatečné, musí být zabezpečeno šifrováním.
25. Opravy ICT komponent mohou být prováděny pouze na základě smluvně ošetřeného vztahu se ZK.
26. Fyzický přístup k prostředkům IS je umožněn pouze druhým smluvním stranám (servisní a dodavatelské organizace, dohody o provedení práce apod.), u kterých udělení přístupu vyplývá z uzavřené smlouvy. Fyzický přístup k prostředkům IS je možné uskutečnit pouze se souhlasem Správce IS nebo vedoucího oddělení informatiky.
27. Pohyb pracovníků druhých smluvních stran v prostorách serverovny (servisní zásah, revize zařízení apod.) je možný pouze v doprovodu odpovědných pracovníků oddělení informatiky nebo jimi pověřených osob.
28. Pro přímé připojení (v prostorech ZK) do IS ZK smí být použita pouze přidělená technika ZK. Připojování cizí techniky do vnitřní sítě ZK je zakázáno. Výjimky povoluje Správce IS.
29. Na přidělenou techniku ZK nesmí být bez souhlasu pověřené osoby nahráván, instalován nebo z ní odebírán žádný software.
30. Při opuštění pracoviště je vždy nutné provést vhodným způsobem jeho zajištění (pracovní stanice, nosiče dat, papírové dokumenty).
31. Přenosná paměťová média musí být vždy uchovávána na bezpečném místě, např. v uzamčené skříni, stolu nebo místnosti. Originální datová média a záložní kopie citlivých souborů musí být ukládány na bezpečném místě, chráněném nejen proti odcizení a zneužití, ale i proti poškození nebo zničení.
32. Pracovní stanice a data na nich uložená musí být chráněna proti odcizení, proti neoprávněnému přístupu a proti poškození nebo zničení.
33. **Ochrana dat a informačních aktiv**
34. Druhá smluvní strana odpovídá za všechna převzatá data (elektronická a tištěná), způsob jejich použití a ochranu před neoprávněným přístupem a zneužitím. Není-li ve smlouvě stanoveno jinak, před ukončením smluvního vztahu druhá smluvní strana vrátí všechna převzatá data a všechny jejich kopie bezpečně zlikviduje.
35. Druhá smluvní strana je do protokolárního předání pracovníkům ZK odpovědná za všechna zpracovávaná aktiva a je povinna je odpovídajícím způsobem zabezpečit.
36. Ukládání pracovních dat je možné pouze na místa, která určí odpovědná osoba.
37. Druhá smluvní strana nesmí zobrazovat, měnit, mazat nebo kopírovat citlivá data, zejména pak osobní údaje, pokud to nesouvisí se schváleným účelem přístupu.
38. Vadná zařízení (včetně pevných disků) s nešifrovanými citlivými daty mohou být předány externím servisním specialistům pouze po schválení Správcem IS nebo vedoucím oddělení informatiky.
39. Pokud druhá smluvní strana při práci v IS ZK přijde do styku s osobními údaji dle platné legislativy nebo jinými neveřejnými informacemi, je povinna o zjištěných skutečnostech zachovávat mlčenlivost a zajistit jejich utajení.
40. Nepotřebná data (elektronická, na mediích i papírová) musí být vždy neprodleně skartována.
41. Všechny zásahy na serverech musí být předem odsouhlaseny Správcem IS a zaznamenány stanoveným způsobem.
42. **Ochrana proti škodlivým kódům**
43. Pokud je to možné, jsou servery a pracovní stanice vybaveny antivirovým skenerem.
44. Pokud některé aplikace nabízejí možnost zvýšené ochrany, musí být odpovídajícím způsobem nastavena. Způsob nastavení schvaluje Správce IS.
45. Nebezpečné typy souborů jsou blokovány na hranicích bezpečnostního perimetru. Výjimky schvaluje v řádně odůvodněných a zdokumentovaných případech Správce IS.
46. Druhá smluvní strana je povinna dodržovat zásady ochrany proti virům a škodlivým kódům nejen pro nastavení a využívání prostředků ZK, ale i na přístupových bodech a zařízeních druhé smluvní strany.
47. **Bezpečnostní incidenty**
48. Druhá smluvní strana je povinna neprodleně hlásit odpovědným osobám k IS ZK porušení těchto pravidel, všechny zjištěné neobvyklé události, které jsou, nebo mohou být bezpečnostními incidenty, zjištěná zranitelná místa, nedostatky a nesoulady. Při jejich prošetřování a odstraňování je povinna poskytnout účinnou součinnost.
49. Druhé smluvní straně není povoleno řešení bezpečnostních incidentů a odstraňování nedostatků či nesouladů vlastními silami bez předchozího schválení Správcem IS.
50. **Používání internetu**
51. Druhá smluvní strana může používat při práci v IS ZK internet pouze pro účely plnění smlouvy a za podmínky dodržování všech všeobecně uznávaných bezpečnostních pravidel, platných pro práci s internetem. Stahování souborů, používání FTP a jiných služeb je možné jen po dohodě se Správcem IS.
52. Pokud není ve smlouvě stanoveno jinak, není povoleno využívat elektronickou korespondenci z prostředí ZK.
53. **Tisk**
54. Druhá smluvní strana může tisknout na tiskárnách ZK pouze s povolením odpovědné osoby. Tisknout je povoleno pouze dokumenty související s předmětem smlouvy a při tisku je nutno šetřit spotřební materiál.
55. Tištěné dokumenty musí být zabezpečeny proti neoprávněnému přístupu jak během tisku, tak i po jeho vytisknutí, až do jejich bezpečné skartace.
56. **Použití kryptografických technik**
57. Kryptografické metody musí být použity vždy, jestliže není možné bezpečnost dat nebo komunikace zaručit jinými způsoby. Jedná se např. o přenosy citlivých dat prostřednictvím nedůvěryhodných sítí nebo přístup externích subjektů k citlivým zdrojům.
58. Použity mohou být pouze takové kryptografické algoritmy a protokoly a v takovém užití (např. odpovídající délky klíčů), které jsou podle platných standardů všeobecně považovány za bezpečné.
59. Použití proprietárních nebo obecně neuznávaných algoritmů není dovoleno, výjimky povoluje Správce IS.