SMLOUVA O DÍLO

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

1.

Kraj Vysočina

se sídlem:	Žižkova 1882/57, 586 01 Jihlava
zastoupený:	Ing. Martinem Kuklou, hejtmanem kraje
IČO:	708 90 749
DIČ:	CZ70890749
ID datové schránky:	ksab3e
bankovní spojení:	Komerční banka, a.s.
číslo účtu:	123-6403810267/0100

(dále jen „**Objednatel**“)

a

2.

Aricoma Systems a.s.

se sídlem:	Hornopolní 3322/34, 702 00 Ostrava
zastoupená:	Ing. Jaroslav Dvořák, člen představenstva
IČO:	04308697
DIČ:	CZ04308697
ID datové schránky:	a5udbhc
bankovní spojení:	Česká spořitelna, a.s.
číslo účtu:	6563752/0800

Zapsaná v obchodním rejstříku vedeném u Krajského soudu v Ostravě, sp. zn. B.11012.
(dále jen „**Zhotovitel**“)

Čl. I

Účel a předmět smlouvy

1. Účelem této smlouvy je úprava stávajícího produktu IAM Platforma Aricoma ID, dříve známá jako AC Identita, na který má Kraj Vysočina zakoupenou licenci, užívá jej od roku 2013 a má provedenu integraci vůči cca 50ti systémům a službám kraje, dle tabulky v příloze č.1.
2. Předmětem této smlouvy je závazek Zhotovitele za podmínek stanovených touto smlouvou dodat rozšíření modulů Access Management (AM) a Privileged Identity/Access Management (PIMPAM) do prostředí Objednatele (dále jen „***Dílo***“), poskytnout Objednateli nevýhradní licenci k užití Díla a převést vlastnické právo k nosičům dat, na kterých bude Dílo zpřístupněno Objednateli, a závazek Objednatele Dílo převzít a zaplatit za něj Zhotoviteli cenu sjednanou v čl. IV této smlouvy.
3. Bližší specifikace Díla včetně cenové kalkulace je uvedena v **Příloze č. 1, 2 a 3 této smlouvy**.

Čl. II

Práva a povinnosti smluvních stran

1. Zhotovitel se zavazuje provést pro Objednatele Dílo specifikované v čl. I této smlouvy za podmínek stanovených touto smlouvou.
2. Zhotovitel poskytuje touto smlouvou Objednateli nevýhradní licenci na jakékoli v současnosti známé užití Díla, a to na dobu trvání majetkových autorských práv. Územní rozsah licence bude neomezený. Odměna za poskytnutí licence je součástí ceny sjednané v čl. IV této smlouvy. Licence bude poskytnuta ode dne předání Díla Zhotovitele Objednateli. Objednatel nebude povinen licenci využít. Zhotovitel se zavazuje převést vlastnické právo k nosičům dat, na kterých bude Dílo zpřístupněno Objednateli.
3. Zhotovitel se zavazuje v rámci plnění této smlouvy nevyužívat v rozsahu vyšším než 10 % ceny poddodavatele, který je:
   a) fyzickou či právnickou osobou nebo subjektem či orgánem se sídlem v Rusku,

b) právnickou osobou, subjektem nebo orgánem, který je z více než 50 % přímo či nepřímo vlastněn některým ze subjektů uvedených v písmeni a) tohoto odstavce, nebo

c) fyzickou nebo právnickou osobou, subjektem nebo orgánem, který jedná jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b) tohoto odstavce.

4. Objednatel se zavazuje Dílo převzít a zaplatit za něj cenu sjednanou v čl. IV odst. 1 této smlouvy.

5. Smluvní strany se zavazují informovat se navzájem o všech skutečnostech, které mají, nebo by mohly mít vliv na plnění této smlouvy.

6. Smluvní strany jsou povinny poskytovat si nezbytnou součinnost k plnění této smlouvy.

Čl. III

Doba a místo plnění

1. Místem plnění je sídlo Objednatele na adrese: Žižkova 57, Jihlava.

2. Zhotovitel je povinen Dílo řádně dodat Objednateli nejpozději do 23. 5. 2025 na testovací prostředí a nejpozději do 6. 6. 2025 na produkční prostředí.

3. Řádné a včasné dodání Díla bude potvrzeno předávacím protokolem, který bude obsahovat zhodnocení prací a případně také soupis zjištěných vad a nedodělků, a to spolu s termínem pro jejich odstranění. Předávací protokol bude podepsán kontaktními osobami obou smluvních stran.

4. Objednatel je povinen Dílo převzít za předpokladu, že je řádně a včas dokončené, odpovídá této smlouvě a je prosté vad a nedodělků s výjimkou takových vad a nedodělků, které nebrání řádnému užívání Díla.

5. Právo k užívání Díla přechází na Objednatele zaplacením sjednané ceny Zhotoviteli.

Čl. IV

Cena

1. Smluvní strany se dohodly, že celková cena za dílo činí 968 000,- Kč bez DPH, tzn. aktuálně 1 171 280,- Kč včetně DPH 21%.

2. Ke sjednané výši cen bude účtována DPH ve výši dle právních předpisů účinných ke dni uskutečnění zdanitelného plnění. Dnem uskutečnění zdanitelného plnění je den podpisu předávacího protokolu.

3. Smluvní strany se dohodly, že v případě změny zákonné sazby DPH uvedené v ceně nebudou uzavírat písemný dodatek na změnu ceny a DPH bude účtována podle předpisů platných v době uskutečnění zdanitelného plnění.

Čl. V

Platební podmínky

1. Cena bude uhrazena na základě faktury - daňového dokladu vystaveného Zhotovitelem. Zhotovitelem předložená faktura bude mít splatnost 14 dnů ode dne prokazatelného doručení Objednateli.

2. Zaplacením se pro účely této smlouvy rozumí odepsání příslušné částky z účtu Objednatele ve prospěch účtu Zhotovitele. Účet Zhotovitele uvedený v záhlaví smlouvy je správcem daně (finančním úřadem) zveřejněn způsobem umožňujícím dálkový přístup ve smyslu ustanovení § 109 odst. 2 písm. c) zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „***zákon o DPH***“). V případě, že v době platby tento účet nebude zveřejněn u správce daně, zaplatí Objednatel cenu na jiný účet Zhotovitele, který bude zveřejněn v souladu s § 109 odst. 2 písm. c) zákona o DPH.

3. Faktura musí obsahovat náležitosti daňového dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a zákona o DPH.

4. Faktura bude obsahovat název a reg. číslo projektu CZ.06.01.01/00/22_009/0003523 - Elektronické služby Kraje Vysočina 2023.

5. Fakturu, která neobsahuje uvedené náležitosti, nebo jsou-li tyto 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.

6. Pokud se po dobu účinnosti této smlouvy Zhotovitel stane nespolehlivým plátcem ve smyslu ustanovení § 109 odst. 3 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 Zhotoviteli.

Čl. VI

Kontaktní osoby

1. Kontaktní osobou Zhotovitele je:

   Ing. Jiří Gruss, e-mail: jiri.gruss@aricoma.com, tel.: 606 781 698

2. Kontaktní osoba Objednatele ve věcech technických je:

   Jaroslav Krotký, e-mail: krotky.j@kr-vysocina.cz, tel.: 724 650 193

3. Změnu kontaktních osob a jejich údajů lze provést ve formě jednostranného písemného oznámení bez nutnosti uzavírání dodatku k této smlouvě, přičemž tato změna nabývá účinnosti dnem doručení takového oznámení druhé smluvní straně. Kontaktní osoby slouží pouze pro realizační komunikaci, nejsou oprávněny za smluvní strany právně jednat ve smyslu této smlouvy, nemohou tuto smlouvu měnit, uzavírat k ní dodatky, činit objednávky víceprací apod., pokud k tomu nebudou výslovně písemně zmocněny danou smluvní stranou.

Čl. VII

Vlastnické právo a nebezpečí škody

1. Vlastnické právo k části Díla, která není autorským dílem 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***"), přechází na Objednatele jeho předáním Zhotovitelem v místě plnění. Objednatel zůstává vlastníkem Díla i v případě zániku závazku z této smlouvy jinak než splněním, např. odstoupením některé ze smluvních stran od této smlouvy.

2. Nebezpečí vzniku škody na Díle nese Zhotovitel. Nebezpečí škody na Díle přechází na Objednatele okamžikem oboustranného podpisu předávacího protokolu.

3. Zhotoviteli na základě této smlouvy nevzniká žádné právo na užití dat zpracovávaných prostřednictvím Díla.

Čl. VIII

Odpovědnost za škodu

1. Smluvní strany odpovídají za škodu způsobenou porušením povinností vyplývajících z této smlouvy nebo z obecně závazného právního předpisu.

2. Náhrada škody se řídí § 2913 a násl. občanského zákoníku.

Čl. IX

Záruční podmínky

1. Zhotovitel poskytuje Objednateli na Dílo řádně dodané v souladu s podmínkami této smlouvy záruku za jakost díla v délce 24 měsíců od jeho protokolárního převzetí Objednatelem. V případě, že bylo Dílo předáno s drobnými vadami a nedodělky, jež nebrání řádnému užívání díla, počíná záruční doba běžet ode dne odstranění těchto vad a nedodělků.

2. Zhotovitel poskytuje záruku na celé Dílo a všechny jeho součásti po celou dobu trvání záruční doby, včetně sjednaných technických parametrů.

3. Záruka se vztahuje na všechny vady včetně bezpečnostních zranitelností s bodovým ohodnocením 6.9 a více bodů dle obecného systému hodnocení zranitelností (CVSSv3.1 base score), s výjimkou vad Díla, které jsou způsobeny výlučně Objednavatelem nebo třetími osobami.

4. Zhotovitel je povinen záruční vady odstranit nejpozději do 10 kalendářních dnů od jejich oznámení Objednatelem servisnímu středisku Zhotovitele, nebude-li mezi smluvními stranami písemně dohodnut jiný termín pro odstranění vad.
5. Servisní středisko Zhotovitele pro hlášení závad je v ARICOMA SYSTEMS a.s.
    - RC/Divize Jihlava
    - https://servicedesk.aricoma.com
    - +420 910 971 595, +420 596 152 595
    - sd_vc@aricoma.com
6. Zhotovitel provede o každém servisním zásahu písemný záznam, který předá Objednateli a nechá si ho od něj potvrdit.

Čl. X

Prodlení, sankce

1. Jestliže je Objednatel v prodlení s plněním povinnosti podle této smlouvy, je Zhotovitel oprávněn vyúčtovat a Objednatel povinen zaplatit smluvní pokutu ve výši 500,- Kč za každý i započatý den prodlení. Smluvní pokuta je splatná vždy k poslednímu dni příslušného kalendářního měsíce.
2. V případě, že je Zhotovitel v prodlení s plněním povinností podle této smlouvy, je Objednatel oprávněn vyúčtovat a Zhotovitel povinen zaplatit smluvní pokutu ve výši 1 000,- Kč za každý i započatý den prodlení. Smluvní pokuta je splatná vždy k poslednímu dni příslušného kalendářního měsíce.
3. V případě, že Zhotovitel je v prodlení s odstraněním závad podle čl. IX této smlouvy, je Objednatel oprávněn vyúčtovat a Zhotovitel povinen zaplatit smluvní pokutu ve výši 500,- Kč za každý i započatý den prodlení.
4. Zhotovitel odpovídá za veškeré škody a nemajetkové újmy, které vzniknou Objednateli v důsledku porušení této smlouvy Zhotovitelem. Zhotovitel je povinen nahradit takto vzniklou škodu a nemajetkovou újmu v plném rozsahu, včetně případných sankcí udělených Objednateli orgány veřejné moci, jejichž příčinou bylo porušení povinností Zhotovitele dle této smlouvy.

Čl. XI

Platnost a změna smlouvy

1. Tato smlouva nabývá platnosti dnem podpisu oprávněnými zástupci obou smluvních stran 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. Obsah Smlouvy může být měněn jen dohodou stran, a to vždy jen vzestupně číslovanými písemnými dodatky podepsanými oprávněnými osobami smluvních stran.
4. Kterákoliv ze smluvních stran je oprávněna tuto smlouvu vypovědět, a to bez udání důvodů. Výpovědní lhůta činí 2 měsíce a začíná běžet první den měsíce následujícího po prokazatelném doručení výpovědi druhé smluvní straně.
5. Objednatel má právo vypovědět tuto smlouvu v případě, že v souvislosti s plněním účelu této smlouvy dojde ke spáchání trestného činu. Výpovědní doba činí 3 dny a začíná běžet dnem následujícím po dni, kdy bylo písemné vyhotovení výpovědi doručeno Zhotoviteli.
6. Pokud se Zhotovitel stane subjektem ve smyslu ustanovení článku 5k Nařízení Rady (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, v aktuálním znění, je Objednatel oprávněn od smlouvy odstoupit v okamžiku, kdy mu bude tato skutečnost známa. Odstoupení nabývá účinnosti dnem doručení Zhotoviteli.
7. Tuto smlouvu lze rovněž ukončit písemným odstoupením Objednatele, který je oprávněn (kromě případů uvedených v § 2001 a násl. občanského zákoníku) od této smlouvy písemně odstoupit, byl-li pravomocně zjištěn úpadek Zhotovitele a rozhodnuto o způsobu řešení úpadku konkursem, nebo byl-li insolvenční návrh pravomocně zamítnut pro nedostatek majetku Zhotovitele.

Čl. XII

Bezpečnostní ustanovení

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. Příloha č. 3 je aktuální k datu podpisu smlouvy, Informace v příloze č. 3, především bezpečnostní politiky, se mohou v čase měnit. Pokud dojde ke změnám informací v příloze č. 3, bude příloha č. 3 změněna a nahrazena aktuálními informacemi a bezpečnostními politikami. Zhotovitel má právo v případě implementace nových bezpečnostních opatření, řešit implementaci bezpečnostních opatření jako placený rozvoj, a to formou objednávky nebo dodatkem k této smlouvě s Objednatelem.
3. Zhotovitel je povinen zajistit plnění bezpečnostních opatření a požadavků stanovených touto smlouvou ve stejné míře u všech případných subdodavatelů či 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. 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 50 000,- Kč, a to za každé jednotlivé porušení povinností obsažených v tomto článku

Čl. XIII

Závěrečná ustanovení

1. Výběr Zhotovitele byl proveden v souladu s Pravidly Rady Kraje Vysočina pro zadávání veřejných zakázek ze dne 29. 6. 2021.
2. Zhotovitel prohlašuje, že se před uzavřením smlouvy nedopustil v souvislosti se zadávacím řízením 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 smlouvu, a že se zejména ve vztahu k ostatním uchazečům 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. Vztahy smluvních stran touto smlouvou blíže neupravené se řídí příslušnými ustanoveními občanského zákoníku s přihlédnutím k příslušným ustanovením autorského zákona.
5. Tato Smlouva se uzavírá elektronickou formou, přičemž obě smluvní strany obdrží její elektronický originál opatřený uznávanými, resp. kvalifikovanými elektronickými podpisy osob zastupujících obě smluvní strany. V případě, že Smlouva nebude uzavřena elektronickou formou, bude vyhotovena v počtu dvou (2) stejnopisů, opatřena vlastnoručními podpisy osob zastupujících obě smluvní strany, z nichž každá smluvní strana obdrží po jednom.
6. 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.
7. Zhotovitel výslovně souhlasí se zveřejněním celého textu této smlouvy, včetně podpisů, v Registru smluv. 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.

V Jihlavě dne ……

Ing. Jaroslav Dvořák

Digitálně podepsal Ing. Jaroslav Dvořák
Datum: 2025.04.16 11:43:21 +02'00'

Za Zhotovitele
Ing. Jaroslav Dvořák

V Jihlavě dne …….

Ing. Martin Kukla
Kraj Vysočina
17.4.2025 07:36:18 +02:00

Za Objednatele
Ing. Martin Kukla

Příloha č. 1 – Bližší specifikace Díla včetně cenové kalkulace

úprava stávajícího produktu IAM Platforma Aricoma ID, dříve známá jako AC Identita, na který má Kraj Vysočina zakoupenou licenci, užívá jej od roku 2013 a má provedenu integraci vůči cca 50ti systémům a službám kraje.

Položka kalkulace	**Cena za kus v Kč bez DPH**	**Počet ks**	**Celkem za položku v Kč bez DPH**	**Celkem za položku v Kč s DPH**
Rozvoj systému pro správu elektronických identit v níže uvedených modulech: - Access Management (AM) - Privileged Identity/Access Management (PIMPAM)	968 000,- Kč	1	968 000,- Kč	1 171 280,- Kč
Celkem	**968 000,- Kč**	**1**	**968 000,- Kč**	**1 171 280,- Kč**

Příloha č. 2: Technická specifikace

Rozvoj systému pro správu elektronických identit
Modul: Access Management (AM)

Obecné

- Autentizace pomocí protokolů SAML2 a OpenID Connect
- Synchronizace AC Identita IDM (uživatelé, aplikace, aplikační role)
- Možnost připojení obecných poskytovatelů identit Idp Google, Facebook
- Možnost zobrazení jednotlivých Idp jako panely/tlačítka (místo rozevíracího seznamu)
- Napojení logů autentizační brány na SIEM (syslog)

Administrace (IDM GUI modul AM)

- Možnost nastavení úrovně logování – WARN/ERROR/DEBUG
- Emailová komunikace autentizační brány (ověřování údajů přes email, notifikace – nastavení SMTP serverů přímo v GUI administrace)
- Service provider (SEP)
    - Vlastní konfigurační parametry pro daný SEP
    - Vazba na vlastní Groovy skripty pro daný SEP – možnost změny response pro SEP
    - Zobrazení aplikačních rolí z IDM – vazba SEP-Aplikace
    - Souhlasové formuláře
    - Správa certifikátů pro daný SEP (šifrování, podpis)
    - Zobrazení uživatelů přihlášených do daného SEPu
- Identity provider (IDP)
    - Vlastní konfigurační parametry pro daný IDP
    - Vazba na vlastní Groovy skripty pro daný IDP – možnost změny request pro IDP
    - Správa certifikátů pro daný IDP (šifrování, podpis)
- Možnost definovat jednotlivé Idp pro dané Sepy
- Správa certifikátů použitých v rámci celé autentizační brány
- Správa aplikačních rolí v rámci celé autentizační brány
- Definování atributů služeb použitých pro jednotlivé SEPy
- Definování specifických souhlasových formulářů pro jednotlivé SEPy
- Správa uživatelů autentizační brány včetně všech session/přihlášení
- Odstranění nutnosti ručního přenačítání konfigurace z IDM GUI – modul AM do AM databáze
- Historie a systémové informace u všech objektů autentizační brány

Klientský portál Autentizační brány Kraje Vysočina

- Možnost si zobrazit profil tzn. „Můj profil" se všemi údaji o své osobě
- Možnost zobrazení důvěryhodnosti údajů (ověřený údaj, důvěryhodný údaj, nedůvěryhodný údaj)
- Možnost doplnit adresu a kontaktní údaje (soukromý email a mobilní telefon)
- Možnost získat souhlas s uchováním osobních údajů na autentizační bráně
- Možnost správy udělených souhlasů na poskytování daných údajů pro jednotlivé aplikace (zobrazení souhlasů tzn. od-od, aplikace, typ souhlasu jednorázový/trvalý, odebrání souhlasu)
- Možnost spravovat připojené účty (odebrat vazbu na jednotlivé poskytovatele identity (Idp))
- Možnost jazykové mutace v anglickém jazyce

Modul: Privileged Identity/Access Management (PIMPAM) technická specifikace

Modul PIMPAM bude sloužit k řízení, správě, monitoringu a zabezpečení privilegovaných účtů na platformách MS Windows a Unix-like OS (FreeBSD, Linux).
Použití modulu na platformách v níže uvedených verzích:

- MS Windows (včetně následných vydaných verzí a edic MS Windows Server a MS SQL Server)
    - Windows Server 2016
    - Windows Server 2019
    - Windows Server 2022
- Unix-like (vždy v aktuálních stabilních verzích popř. TLS)
    - GNU/Linux v různých distribucích (Debian, CentOS, RedHat, Ubuntu apod.)
    - FreeBSD

Požadavky na modul:

- Dodávka modulu nebude omezovat:
    - počet uživatelů
    - počet řízených koncových serverů/systémů/aplikací
    - počet řízených účtů
- Modul musí umožnit ukládání a přenos autentizačních prostředků (hesel, klíčů) ve vlastní bezpečné komponentě. Bezpečnost komponenty musí být založena na silných kryptografických protokolech, algoritmech a klíčích, přičemž požadavky na kryptografii jsou uvedeny níže
- Modul musí umožnit pracovat administrátorům ICT pod jednou identitou a té na základě definovaných politik zpřístupňovat koncové systémy pod definovanými doménovými privilegovanými či doménovými systémovými účty a tím pádem zabránit administrátorům ICT přímému přístupu k autentizačním prostředkům účtů na koncových systémech.
- Modul musí umožnit připojení k cílovým systémům prostřednictvím minimálně těchto protokolů a způsobů: RDP, SSH, Remote Application přes RDP
- Logování
    - Modul musí umožnit logování činností minimálně v tomto rozsahu:
        - Přihlášení a odhlášení všech uživatelů včetně neúspěšných pokusů – jak do modulu samotného, tak do koncových systémů
        - Činnosti provedené administrátory Modulu
            - přidělení/odebrání/reset oprávnění
            - založení/smazání/ uživatele či přidělení/odebrání role
            - vytvoření/změna/smazání politiky
            - změna způsobu logování
            - neprovedení operací v důsledku nedostatečných oprávnění
            - změna hesel
        - Činnosti provedené uživateli modulu
            - Zobrazení hesel
            - Nahrávání činností ICT administrátorů (uživatelů modulu) na koncových zařízeních – požadavky zmíněny výše v této dokumentaci.
    - zaznamenané události musí obsahovat minimálně tyto informace:
        - přesný datum a čas vzniku události
        - název aplikace/modulu, kterého se událost týká
        - typ události
        - původce události
        - úspěch/neúspěch události
    - Modul musí umožnit zasílat logy do monitorovacího nástroje SIEM
- Webový server musí být nakonfigurován tak, aby zajišťoval maximální možnou míru bezpečnosti informací 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
- Cross-Origin-Opener-Policy
    - Musí být implementována
- Cross-Origin-Resource-Policy
    - Musí být implementována

Oblasti provozní dokumentace

Záloha, obnova, restart
Cíl dokumentu: popsat a zdokumentovat strategii zálohování systému, jakým způsobem, kdy, kam a jak často jsou zálohována data v rámci daného informačního 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) a disaster recovery plánu, textový popis, návodné obrázky, okomentované příkazy, apod.
- 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
        - Včetně potřebných zdrojů, jako je např. SW, HW, přístupové údaje, data, parametry disaster recovery prostředí, apod.
- 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 (pořadí konkrétních procesů, služeb, apod.), způsob základní kontroly funkčnosti, výčet služeb, které je potřeba spustit/zkontrolovat, apod.

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

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

Příloha č. 3 – Požadavky na bezpečnost informací a kryptografii

Objednatel si vyhrazuje právo na provedení kontroly či zákaznického auditu plnění vybraných požadavků a ustanovení u zhotovitele, přičemž za vybraná ustanovení jsou považována všechna uvedená v příloze č. 3 této smlouvy.

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.

Bezpečné vývojové prostředí

Zhotovitel se zavazuje dodržovat tato pravidla bezpečného vývoje:

- 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 dodavatele/výrobce informačního aktiva či zhotovitele díla.
- Přístupy ke zdrojovým kódům 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.
- Zdrojové kódy systému musí být řádně dokumentovány.
- API rozhraní musí být dokumentováno ve strojově zpracovatelném formátu dle některého z otevřených standardů (např. Swagger OPENAPI).

Řízení kybernetických bezpečnostních incidentů:

Zhotovitel je povinen objednateli hlásit veškeré kybernetické bezpečnostní incidenty, které by mohli mít nějakou souvislost s dílem, s informacemi objednatele či s prováděním této smlouvy.

Zhotovitel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy Kraje Vysočina.

Kryptografie

Pokud budou v souvislosti s touto smlouvou nebo v Díle použity kryptografické prostředky, funkce či algoritmy, musí splňovat následující relevantní minimální požadavky.

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.

Hashovací funkce

Ukládání otisků hesel

- pro ukládání hesel uživatelů mohou být použity pouze tyto tzv. pomalé hashovací funkce:
  - Argon2 s parametry alespoň t=1, m=2^{21}, p=4 a funkcí Argon2id
  - scrypt s parametry alespoň N= 131072 (2^{17}), r=8, a p=1
  - PBKDF2 – variantní řešení:
    - HMAC-SHA-256 s počtem iterací alespoň 600 000
    - HMAC-SHA-512 s počtem iterací alespoň 210 000
- při hashování každého 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 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)
- délka otisku 384 bitů a vyšší

Ověřování integrity souborů

- SHA-2 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)
- délka otisku 384 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) - 3072 bitů
            - pro Elliptic Curve Diffie-Hellman (ECDH) – 256 bitů a více
        - nesmí být použita anonymní výměna klíčů
    - algoritmy a funkce pro autentizaci
        - minimální délky klíčů:
            - RSA - 3072 bitů
            - DSA – 3072 bitů
            - ECDSA - 256 bitů
    - algoritmy a funkce pro symetrické šifrování
        - nesmí být použita hodnota NULL v cipher suites
        - nesmí být použity tyto šifry:
            - DES, 3DES, RC4
        - minimální délka šifrovacího klíče - 128 bitů
        - cipher suites s šiframi s větší délkou klíče musí mít větší prioritu v seznamu ciphersuites než s menší délkou klíče
    - MAC (Message Authentication Code)
        - použití SHA funkce s minimální délkou hashe 256 bitů
        - vyšší délky otisků musí mít vyšší prioritu v cipher suites

TLS cipher suites

- Doporučené cipher suites (v doporučeném pořadí), které naplňují výše zmíněné požadavky
- TLS1.3:
  TLS_AES_256_GCM_SHA384
  TLS_CHACHA20_POLY1305_SHA256
  TLS_AES_128_GCM_SHA256
  TLS_AES_128_CCM_SHA256

- TLS1.2:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Šifrování, podepisování a autentizace

- týká se různých technologií PKI, PGP, S/MIME, SSH, apod.
- minimální délka klíče
    - algoritmus DSA – 3072 bitů
    - algoritmus RSA - 3072 bitů
    - algoritmus ECDSA - 256 bitů
- Ověřování (např. SSH klíče)
    - délka klíče minimálně 3072 bitů u RSA a DSA algoritmů
    - 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