**Příloha č. 3 smlouvy: Seznam SW**

V této příloze je v souladu s článkem I. uveden SW, který je nainstalován na výpočetní technice, předané nájemci. K tomuto SW pronajímatel vlastní příslušné licence.

|  |
| --- |
| Popis licence |
| Windows 10 Pro |
| Kaspersky Anti-Virus Suite |
| CARDPAY 2.9.2 |
| MS Office 2016 |

**Bezpečnostní pravidla pro práci v informačním systému (IS) Zlínského kraje (ZK)**

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 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 subdodavatelů, 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 odboru informačních a komunikačních technologií.
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 smluvní pokutou.
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. 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 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 zabezpečena 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 odboru informačních a komunikačních technologií.
27. Pohyb pracovníků druhých smluvních stran v prostorách serverovny (servisní zásah, revize zařízení apod.) je možný pouze v doprovodu odpovědných pracovníků odboru informačních a komunikačních technologií 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 odboru informačních a komunikačních technologií.
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 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.

**SMLOUVA O MLČENLIVOSTI, OCHRANĚ INFORMACÍ**

**a souhlasu s dodržováním bezpečnostních pravidel v souvislosti s předáním přihlašovacích údajů**

uzavřená na základě ust. § 1746 odst. 2 zákona č. 89/2012 Sb. Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“)

**Smluvní strany**

**Předávající: Zlínský kraj**

Adresa: třída Tomáše Bati 21, 761 90 Zlín

IČ: 70891320

DIČ: CZ70891320

Zastoupený: Ing. Petr Kedra, vedoucí odboru KŘ

Bankovní spojení: Česká spořitelna, a.s., č.ú. 2786182/0800

a

**Přejímající: HP TRONIC, s.r.o.**

Adresa: náměstí Práce 2523, 760 01 Zlín

IČ: 60323418

DIČ: CZ60323418

Zapsaný v OR: Krajským soudem v Brně, oddíl C, vložka 38954

Zastoupený: Ing. Danielem Večeřou, jednatelem

Bankovní spojení: 17527343/0300

(dále společně jen jako„Smluvní strany“).

**Článek 1
Předmět Smlouvy**

* 1. Účelem této Smlouvy je ochrana důvěrných informací Předávajícího, se kterými se Přejímající seznámí v rámci spolupráce (dále též jako „vzájemná spolupráce“) nebo přístupu do informačních systémů nebo do prostor Předávajícího.
	2. Předávající předává Přejímajícímu přihlašovací údaje a přístupy do prostor nebo informačních systémů Předávajícího uvedené v Příloze č. 2 této Smlouvy o mlčenlivosti, ochraně informací a souhlasu s dodržováním bezpečnostních pravidel v souvislosti s předáním přihlašovacích údajů (dále jen „Smlouva“). Tyto přihlašovací údaje a přístupy jsou určeny pro plnění smluvních závazků vyplývajících ze Smlouvy o provozování stravovacího zařízení a poskytování souvisejících služeb.
	3. Předmětem této Smlouvy je bližší vymezení bezpečnostních pravidel v souvislosti s předáním přihlašovacích údajů do informačních systémů nebo přístupů do prostor Předávajícího, které musí Přejímající dodržovat po dobu platnosti přihlašovacích údajů do informačních systémů nebo přístupů do prostor Předávajícího.
	4. Předmětem této Smlouvy je bližší vymezení důvěrných informaci Předávajícího a převzetí závazku Přejímajícího zachovat o těchto důvěrných informacích mlčenlivost a nesdělit je ani neumožnit k nim přístup třetím osobám, nebo je nevyužít ve svůj prospěch nebo ve prospěch třetích osob, není-li v této Smlouvě stanoveno jinak.

**Článek 2
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 Přejímající v průběhu vzájemné spolupráce dozví, a/nebo které mu Předávající v průběhu vzájemné spolupráce zpřístupní (dále jen „důvěrné informace“).
	2. Důvěrné informace touto Smlouvou chráněné tvoří rovněž veškeré skutečnosti technické, ekonomické, právní a výrobní povahy v hmotné nebo nehmotné formě, které byly Předávajícím takto označeny a byly poskytnuty Přejímajícímu. Důvěrné informace mohou být dále společně označeny též jako „chráněné informace“.
	3. Přejímající 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. Předávající má právo požadovat doložení dostatečnosti utajení důvěrných informací. Přejímající 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 Přejímající 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 Předávajícího a informace Předávajícího, pro nakládání s nimiž je stanoven právními předpisy zvláštní režim utajení (zejména hospodářské tajemství, státní tajemství, bankovní tajemství, služební tajemství). Dále se považují za důvěrné informace takové informace, které jsou jako důvěrné výslovně Předávajícím označeny.
	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 Předávajícím, pokud je Přejímající schopen tuto skutečnost doložit, a konečně informace poskytnuté třetí osobou, která takové informace nezískala porušením povinnosti jejich ochrany.
	7. Přejímající 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 Předávající přestane utajovat; v pochybnostech se má za to, že utajování informací trvá.
	9. Po ukončení účinnosti této Smlouvy je Přejímající povinen bez zbytečného odkladu vrátit Předávajícímu všechny poskytnuté materiály obsahující důvěrné informace včetně jejich případně pořízených kopií. O předání a převzetí se sepíše protokol podepsaný oběma smluvními stranami.
	10. Smluvní strany se zavazují, že obchodní a technické informace, které jim byly svěřeny druhou stranou, nezpřístupní třetím osobám bez písemného souhlasu druhé strany a nepoužijí tyto informace k jiným účelům, než k plnění podmínek a účelu této smlouvy. Ustanovení zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, nejsou tímto dotčena.

**Článek 3**

**Zpracování a ochrana osobních údajů**

1. Smluvní strany se zavazují, v souvislosti s touto smlouvou, postupovat v souladu s Nařízením Evropského parlamentu a Rady (EU) č. 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 (dále jen „Nařízení“).
2. Předávající je a bude nadále považován za Správce osobních údajů, se všemi pro něj vyplývajícími důsledky a povinnostmi.
3. Při plnění této smlouvy nepřichází Přejímající do styku s osobními údaji, kterých je Předávající správce (dále jen „chráněné osobní údaje“).
4. Pouze ve výjimečných případech se může stát, že Přejímající získá přístup k chráněným osobním údajům. Pokud se tak stane, jedná se o zpracování z pověření správce dle článku 29 Nařízení.
5. Přejímající se zavazuje zachovávat mlčenlivost o všech chráněných osobních údajích, se kterými přijde do styku v souvislosti s plněním dle této smlouvy. Přejímající se zejména zavazuje:
	1. nesdělovat nebo nezpřístupňovat chráněné osobní údaje třetím stranám bez předchozího souhlasu Předávajícího,
	2. zajistit, že jeho zaměstnanci a další osoby, které přijdou do styku s chráněnými osobními údaji v souvislosti s plněním dle této smlouvy, budou zavázány povinností mlčenlivosti ve stejném rozsahu, v jakém je mlčenlivostí vázán on sám, a aby tato povinnost mlčenlivosti trvala i po skončení jejich zaměstnání nebo provádění prací (minimálně po dobu 1 roku),
	3. zajistit, aby osoby, které se budou podílet na plnění dle této smlouvy, při styku nebo nakládání s chráněnými osobními údaji nepořizovaly kopie chráněných osobních údajů bez předchozího písemného souhlasu Předávajícího a aby jejich činností nebo opomenutím nedošlo k náhodnému nebo protiprávnímu zničení, ztrátě či pozměnění chráněných osobních údajů, nebo k jejich neoprávněnému zpřístupnění třetím osobám.
6. Přejímající je povinen po dobu plnění předmětu smlouvy realizovat potřebná bezpečnostní opatření v rovině technické i organizační, aby zajistil úroveň zabezpečení odpovídající danému riziku, zejm. pak osobní údaje zabezpečit vůči náhodnému či nezákonnému zničení, ztrátě, změně, zpřístupnění neoprávněným stranám, zneužití či jinému způsobu zacházení s osobními daty v rozporu s Nařízením.
7. Přejímající je povinen písemně seznámit Předávajícího s jakýmkoliv podezřením na porušení nebo skutečným porušením bezpečnosti zpracování osobních údajů podle ustanovení této Smlouvy, např.: jakoukoliv odchylkou od udělených pokynů, odchylkou od sjednaného přístupu, plánovaným zveřejněním, upgradem, testy apod., kterými může dojít k úpravě nebo změně zabezpečení nebo ke zpracování osobních údajů, jakýmkoliv podezřením z porušení důvěrnosti, jakýmkoliv podezřením z náhodného či nezákonného zničení, ztráty, změny, zpřístupnění neoprávněným stranám, zneužití či jiného způsobu zacházení s osobními údaji v rozporu s Nařízením.
8. Předávající je oprávněn provádět kontrolu, zda Přejímající plní své povinnosti dle tohoto článku. Přejímající je povinen a zavazuje se k veškeré součinnosti s Předávajícím, o kterou bude požádán v souvislosti s ochranou osobních údajů. Přejímající je povinen na vyžádání zpřístupnit Předávajícímu svá písemná technická a organizační bezpečnostní opatření a umožnit mu případnou kontrolu dodržování předložených technických a organizačních bezpečnostních opatření.
9. Po skončení účinnosti této Smlouvy je Přejímající povinen veškerá data, která má v držení, vymazat, a pokud je dosud nepředal Předávajícímu, předat je Předávajícímu a dále vymazat všechny existující kopie. Pokud má Přejímající přístup k chráněným osobním údajům, má povinnost současně tento přístup deaktivovat či vrátit Předávajícímu. Povinnost uvedená v tomto článku neplatí, stanoví-li právní předpis EU, případně vnitrostátní právní předpis Přejímajícímu data ukládat i po skončení účinnosti této Smlouvy.

**Článek 4
Bezpečnostní pravidla**

* 1. Přejímající se zavazuje dodržovat bezpečnostní pravidla uvedená v Příloze č. 1. této Smlouvy.
	2. Přejímající se zavazuje, že jeho zaměstnanci budou při svých činnostech dodržovat a zachovávat bezpečnostní pravidla uvedena v Příloze č. 1. této Smlouvy.
	3. Přejímající se zavazuje, že seznámí všechny své zaměstnance, kteří budou do informačních systémů nebo do prostor Předávajícího přistupovat s bezpečnostními pravidly před začátkem jakýchkoliv aktivit.
	4. Přejímajícímu je přísně zakázáno vykonávat jiné než dohodnuté činnosti, přistupovat k jiným než povoleným prostředkům, serverům a datům nebo provádět jakékoli úkony směřující k zjišťování rozsahu přidělených oprávnění, dostupnosti jiných síťových prostředků a služeb a způsobech zabezpečení.

**Článek 5
Sankce**

* 1. Za porušení povinností týkajících se ochrany obchodního tajemství, důvěrných informací podle článku 2 nebo osobních údajů podle článku 3 nebo bezpečnostních pravidel dle článku 4 této Smlouvy a přílohy 1 této Smlouvy - článku 1, odst. c) - f), h), čl. 2, odst. a), čl. 3, odst. b), d), čl. 4, odst. e) - g), čl. 5, odst. a), d), e), f), h), čl. 6, odst. d), čl. 7, odst a), b), čl. 8, odst. a), čl. 9, odst. b) a čl. 10, odst. a), b), c) má poškozená smluvní strana právo uplatnit u druhé Smluvní strany, která tyto povinnosti porušila, nárok na zaplacení smluvní pokuty.
	2. Výše smluvní pokuty je stanovena na 10 000,- Kč (slovy: deset tisíc korun českých) za každý jednotlivý prokázaný případ porušení povinností stanovených touto Smlouvou.
	3. Smluvní pokutu, na kterou vznikne poškozené smluvní straně nárok dle této Smlouvy, je druhá smluvní strana povinna uhradit do 30 kalendářních dnů ode dne prokazatelného doručení výzvy k úhradě smluvní pokuty. Má se za to, že řádným doručením druhé Smluvní straně je osobní předání, zaslání prostřednictvím kurýrní služby s poskytnutím potvrzení doručení nebo ověřenou elektronickou zprávou na adresu příslušné smluvní strany.
	4. Doručování prostřednictvím držitele poštovní licence se rozumí, že zpráva je doručována poštovní zásilkou ve formě doporučeného dopisu na doručovací adresu Smluvní strany. Dnem doručení se rozumí den přijetí zásilky nebo také den odmítnutí přijetí zásilky. Dnem doručení se také rozumí třetí (3) den ode dne odevzdání zásilky k poštovní přepravě.
	5. Způsobí-li jedna smluvní strana druhé smluvní straně škodu porušením této Smlouvy, odpovídá za ni dle obecných právních předpisů. Zaplacením smluvní pokuty není dotčen nárok na náhradu škody.

**Článek 6
Audit**

* 1. Přejímající umožní Předávajícímu či třetím osobám zvoleným Předávajícím přístup do prostor Přejímajícího za účelem kontroly, zda plnění bezpečnostních pravidel dle článku 3 je poskytováno v souladu s touto Smlouvou (dále jen „Audit“).
	2. Přejímající je v souvislosti s Auditem povinen poskytnout Předávajícímu veškerou nezbytnou součinnost.
	3. Pokud Audit prokáže, že Přejímající nesplnil své povinnosti vyplývající z této Smlouvy, uplatní se ustanovení článku 5 této Smlouvy.

**Článek 7
Závěrečná ustanovení**

## Tato Smlouva představuje úplnou dohodu Smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou Smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných oprávněnými zástupci obou smluvních stran.

## Obě smluvní strany se zavazují, že vzniklé spory budou řešit přednostně smírčí cestou, jednáním zástupců obou smluvních stran a v souladu s platnými právními předpisy České republiky.

## Zhotovitel se dále zavazuje poskytnout řádnou součinnost při výkonu finanční kontroly v souladu s § 2 písm. e) a § 13 zák. 320/2001 Sb., o finanční kontrole, ve znění pozdějších předpisů, a to z důvodu, že zakázka je hrazena z veřejné finanční podpory.

## Závazkový vztah založený touto Smlouvou se řídí Občanským zákoníkem a Autorským zákonem.

## Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1 Bezpečnostní pravidla

## Tato Smlouva je sepsána ve čtyřech (4) vyhotoveních, z nichž Předávající obdrží tři a Přejímající jedno. Smlouva nabývá platnosti dnem, kdy bude podepsána oběma stranami a účinnosti dnem, kdy bude podepsaná smlouva doručena smluvní stranou, která smlouvu podepsala jako poslední, druhé smluvní straně.

## Tato smlouva je účinná po dobu účinnosti realizační smlouvy.

## Rozhodnout o uzavření této smlouvy a oprávnění uzavřít jménem ZK tuto smlouvu bylo Ing. Petru Kedrovi, vedoucímu odboru Kanceláře ředitele, svěřeno usnesením Rady Zlínského kraje č. 0364/R12/18 ze dne 7. 5. 2018.

|  |  |
| --- | --- |
|  Ve Zlíně dne ………. |  Ve Zlíně dne ……….. |
| .............................................Ing. Petr Kedra Za Předávajícího | .............................................Ing. Daniel VečeřaZa Přejímajícího |