Smlouva o dílo

Smluvní strany:

Ostravská univerzita
provozní jednotka: Centrum informačních technologií
se sídlem: Bráfova 5, 702 00 Ostrava - Moravská Ostrava
IČ: 619 88 987
DIČ: CZ61988987
zastoupená: doc. Mgr. Petrem Kopeckým, Ph.D., rektorem
kontaktní osoba ve věcech realizace: Ing. Pavel Pomezný, mob. +420 739 329 097, e-mail: pavel.pomezny@osu.cz
bankovní spojení: ČNB, pobočka Ostrava
číslo účtu: 931761/0710

(dále jen „**objednatel**“)
na straně jedné

a

O2 IT Services s.r.o.
se sídlem: Za Brumlovkou 266/2, Michle, 140 00 Praha 4
IČ: 02819678
DIČ: CZ02819678
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 223566
zastoupena: Ing. Janem Bechyněm, jednatelem a Mgr. Janem Hruškou, jednatelem
kontaktní osoba ve věcech realizace: Martin Dolný, mob. +720757074, e-mail: martin.dolny@o2.cz
bankovní spojení: PPF banka, a.s.
číslo účtu: 2019110006/6000
(dále jen: „**zhotovitel**“)
na straně druhé

uzavřely níže uvedeného dne, měsíce a roku smlouvu o dílo následujícího znění (dále jen „**smlouva**“):

Článek I.
Předmět smlouvy

1. Zhotovitel se zavazuje provést analýzu stavu systému řízení bezpečnosti informací (SŘBI) na Ostravské univerzitě a na základě analýzy a požadavků objednatele uvedených v Příloze smlouvy vytvořit soubor písemných bezpečnostních politik, metodik a bezpečnostní dokumentace. Zhotovitel navrhne konkrétní, prokazatelné a měřitelné výstupy a dokumenty, tak aby objednatel na základě jejich aplikace splňoval všechny povinnosti stanovené zák. č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „**ZKB**"), včetně souvisejících vyhlášek a ostatních obecně závazných dokumentů, to vše pro režim vyšších povinností pro oblast organizačních opatření (dále jen „**dílo**"). Dílo je realizováno v rámci projektu: „Výzkum, inovace, vývoj a transfer na OU" (VIVAT OU), reg. č. CZ.02.01.01/00/23_026/0011432, který je spolufinancován z Operačního programu Jan Amos Komenský.
2. Zhotovitel prohlašuje, že se se zadáním k dílu podrobně seznámil a nemá k němu výhrady. Dále prohlašuje, že má k realizaci díla veškerá potřebná oprávnění v souladu s příslušnými obecně závaznými právními předpisy a zadávací dokumentací k této veřejné zakázce.
3. Objednatel se zavazuje zaplatit za dílo cenu za podmínek níže uvedených.

Článek II.
Podmínky plnění

1. Místem plnění je sídlo objednatele.
2. Objednatel je povinen poskytnout zhotoviteli při implementaci nezbytnou součinnost, zejména je povinen poskytnout mu veškeré vyžádané podklady potřebné pro řádné plnění. V případě pochybností objednatele o potřebnosti těchto podkladů je zhotovitel povinen poskytnout mu písemné vysvětlení.
3. Zhotovitel se zavazuje dílo dokončit nejpozději do 11 měsíců. Zhotovitel se zavazuje předávat dílo postupně, formou dílčích plnění podle harmonogramu uvedeného v Příloze smlouvy (dále jen „**dílčí plnění**").
4. Zhotovitel je povinen vyzvat Objednatele k převzetí dílčího plnění min. 5 pracovních dnů předem, a to formou zaslání e-mailu, který bude obsahovat funkční odkaz do aplikace Microsoft Teams, kde bude kompletní dílčí plnění k dispozici pro nahlédnutí a kontrolu před převzetím. Přístup do aplikace Microsoft Teams objednatel zhotoviteli zpřístupní do 5 pracovních dnů od účinnosti této smlouvy.
5. O předání a převzetí dílčích plnění, jakož i k důvodům odmítnutí převzetí, bude sepsán protokol podepsaný oběma smluvními stranami.
6. Zhotovitel není povinen převzít dílčí plnění, trpí-li vadami a nedodělky. Jakékoliv vady a nedodělky budou uvedeny v předávacím protokolu. Tyto je zhotovitel

povinen odstranit ve lhůtě do 5 pracovních dnů, nedohodnou-li se smluvní strany písemně jinak. Tento scénář se případně bude opakovat do doby, kdy dojde k úplnému odstranění vad a nedodělků.

7. Objednatel je oprávněn provádění implementace průběžně kontrolovat. Zhotovitel je povinen mu za tímto účelem poskytovat na písemnou výzvu informace o stavu plnění, a to do dvou pracovních dnů.

Článek III.
Licenční podmínky. Ostatní ujednání.

1. Objednatel získává na základě této smlouvy výhradní právo k užití díla, bez možnosti udělit podlicenci. Poskytnutá licence je časově a územně neomezená.
2. V případě, že má dojít k jakékoliv změně v oprávnění zhotovitele ve smyslu čl. I bod 2, či v personálním složení ve vztahu k osobám, jejichž prostřednictvím byla prokazována kvalifikace ve výběrovém řízení, je zhotovitel povinen na tuto skutečnost objednatele obratem písemně upozornit. Osobu, jejíž prostřednictvím byla prokazována kvalifikace, je zhotovitel povinen obratem nahradit osobou, která splňuje kvalifikační požadavky min. se zadávací dokumentací. Dotyčná osoba se může do plnění zakázky zapojit poté, kdy splnění těchto požadavků ověří objednatel na základě dokladů předložených zhotovitelem. Objednatel je povinen vyjádřit se k nim písemně do 3 pracovních dnů. Neučiní-li tak, má se za to, že k dokladům nemá výhrady.

Článek IV.
Cena

1. Objednatel se zavazuje uhradit zhotoviteli za plnění podle této smlouvy cenu celkem (dále jen „**cena**“):

bez DPH	363 135,-	Kč
sazba DPH	21%	
DPH	76 258,-	Kč
s DPH	439 393,-	Kč

2. Cena se skládá z položek uvedených v Nabídce zhotovitele.
3. Cenu uhradí objednatel bezhotovostně na účet uvedený v záhlaví této smlouvy.

4. Cena bude uhrazena na základě daňového dokladu – faktury vystavené po předání software. Splatnost faktury se sjednává na 30 dnů ode dne jejího doručení objednateli.
5. Zhotovitel je povinen poslat fakturu elektronickými prostředky na adresu financni.uctarna@osu.cz.
6. Daňový doklad – faktura musí obsahovat všechny náležitosti řádného účetního a daňového dokladu ve smyslu příslušných právních předpisů, zejména zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, jakož i následující informaci o projektu – **„hrazeno z projektu VIVAT OU, reg. č. CZ.02.01.01/00/23_026/0011432“**. V případě, že faktura nebude mít uvedené náležitosti, je objednatel oprávněn ji vrátit ve lhůtě splatnosti zpět zhotoviteli k doplnění, aniž se tak dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného dokladu objednateli.
7. Zhotovitel nemá nárok na zálohu.

Článek V.
Záruka a servisní podpora

1. Zhotovitel poskytne objednateli záruku na řádně provedené dílo v délce 6 měsíců ode dne převzetí posledního dílčího plnění bez vad a nedodělků.
2. Zhotovitel uplatní reklamaci na základě písemného oznámení na e-mail zhotovitele. Zhotovitel je povinen potvrdit přijetí reklamace a vadu odstranit nejpozději do 5 pracovních dnů, nebude-li dohodnuto jinak.
3. Za vadu je díla považován mimo jiné rozpor díla s obecně závaznými právními předpisy, jakož i metodickými pokyny či stanovisky ministerstva vnitra a aktuální rozhodovací praxí soudů a příslušných správních orgánů.

Článek VI.
Smluvní pokuty a náhrada škody.

1. V případě prodlení zhotovitele s dokončením dílčího plnění dle Přílohy smlouvy je objednatel oprávněn požadovat na zhotoviteli zaplacení smluvní pokuty ve výši 1000 Kč, a to za každý i jen započatý den prodlení.
2. V případě prodlení zhotovitele s odstraněním záruční vady, jakož i se splněním jakékoliv povinnosti podle ust. čl. III odst. 2, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 300,- Kč, a to za každý i jen započatý den prodlení.

3. V případě porušení povinností ve vztahu k ochraně důvěrných informací dle čl. VII, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 500.000 Kč, a to za každý jednotlivý případ.
4. V případě prodlení objednatele s úhradou faktury je zhotovitel oprávněn uplatnit vůči objednateli pouze úrok z prodlení ve výši 0,05 % z dlužné částky za každý i jen započatý den prodlení s úhradou faktury.
5. Smluvní pokuty jsou splatné na výzvu, přičemž mají převážně sankční charakter. Zaplacení smluvní pokuty nemá vliv na povinnost nahradit vzniklou škodu, která může být způsobená mj. povinností vrátit dotaci či její část.
6. Náhrada škody je limitována částkou 1 mil. Kč.

Článek VII.
Ochrana důvěrných informací.

1. Zhotovitel bere na vědomí, že objednatel je správcem významných informačních systémů dle ustanovení § 3 písm. e) ZKB. Zhotovitel tímto bere na vědomí, že poskytnutí plnění bude součástí podpůrných aktiv významných informačních systémů. Zhotovitel se zavazuje informovat objednatele bezodkladně o všech skutečnostech, které mohou mít vliv na zabezpečení dodaného předmětu plnění, zejména o všech kybernetických bezpečnostních incidentech či jevech, které je potenciálně mohou způsobit, a dále bezodkladně informovat o všech významných změnách v ovládání zhotovitele (ve smyslu zákona č. 90/2012, Sb., o obchodních korporacích, ve znění pozdějších předpisů).
2. Zhotovitel se zavazuje, že jakkoliv nezneužije či využije v rozporu s touto smlouvou a budou chránit a utajovat před třetími osobami veškeré informace, data či údaje (dále jen „důvěrné informace“), které si vzájemně poskytnou či zpřístupní v rámci plnění této smlouvy, a to v jakékoliv formě a bez časového omezení.
3. Závazek ochrany důvěrných informací se nevztahuje na informace, které smluvní strana získala z veřejně dostupného zdroje (nebo od třetí osoby), a při jejich získání nedošlo k protiprávnímu jednání smluvní strany (nebo této třetí osoby); nebo byly uveřejněny a staly se všeobecně přístupnými veřejnosti bez porušení této smlouvy smluvní stranou; nebo v době zpřístupnění smluvní straně byly této smluvní straně známy bez omezení, což tato smluvní strana může doložit, a při jejich získání nedošlo k protiprávnímu jednání smluvní strany; nebo byly z takové ochrany vyloučeny s předchozím písemným souhlasem Informaci poskytující smluvní strany; nebo je nutné je zpřístupnit podle obecně závazných právních předpisů, či na základě soudního či správního rozhodnutí.

OSTRAVSKÁ UNIVERZITA

Článek VIII.
Závěrečná ustanovení

1. Smlouvu lze měnit a doplňovat pouze písemně, a to vzestupně číslovanými dodatky.
2. Tato smlouva se řídí výhradně právem České republiky a podléhají výhradně příslušnosti soudů České republiky.
3. Smlouva může být vyhotovena buď ve fyzické podobě, nebo v elektronické podobě. Pokud je Smlouva vyhotovena listinné podobě, má 2 stejnopisy, každý s platností originálu.
4. Zhotovitel bere na vědomí, že tato smlouva podléhá uveřejnění dle zákona č. 340/2015 Sb., o registru smluv, a souhlasí s jejím uveřejněním v celém rozsahu. Zhotovitel se zavazuje, že provede uveřejnění této smlouvy v registru smluv, čímž smlouva nabyde účinnosti.
5. Prodávající je povinen umožnit všem subjektům oprávněným k výkonu kontroly projektu, z jehož prostředků je dodávka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu danou právními předpisy ČR k jejich archivaci (zákon č. 563/1991 Sb., o účetnictví, a zákon č. 235/2004 Sb., o dani z přidané hodnoty), min. však do **31.12.2040**. Tyto doklady budou uchovávány způsobem stanoveným příslušnými obecně závaznými právními předpisy. Příslušné subjekty mohou mít na základě předpisů obdobné povahy (např. podle zák. č. 255/2012 Sb., zákon o kontrole) právo přístupu i k těm částem nabídek, smluv a souvisejících dokumentů, které podléhají utajení (např. obchodní tajemství, utajované skutečnosti dle zvláštních právních předpisů). Toto oprávnění se vztahuje i na případné poddodavatele zhotovitele, o čemž je zhotovitel povinen tyto své poddodavatele poučit.
6. Přílohy smlouvy, které jsou její nedílnou součástí:

OSTRAVSKÁ UNIVERZITA

Příloha: Specifikace a harmonogram

V Praze

Za zhotovitele:

Ing. Jan Bechyně

Digitálně podepsal Ing. Jan Bechyně
Datum: 2025.10.15 08:16:17 +02'00'

V Ostravě

Za nabyvatele:

doc. Mgr. Petr Kopecký, Ph.D.

Digitálně podepsal doc. Mgr. Petr Kopecký, Ph.D.
Datum: 2025.10.21 14:19:35 +02'00'

Mgr. Jan Hruška

Digitally signed by Mgr. Jan Hruška
Date: 2025.10.16 16:09:23 +02'00'

Příloha č.1 - Rozsah plnění

Zadání

Dodavatel provede analýzu současného stavu systému řízení bezpečnosti informací (SŘBI) na Ostravské univerzitě (dále také „OU“) a na základě analýzy a požadavků vytvoří soubor písemných bezpečnostních politik, metodik a bezpečnostní dokumentace. Dodavatel navrhne konkrétní, prokazatelné a měřitelné výstupy a dokumenty, které umožní univerzitě splnit všechny povinnosti stanovené novým zákonem o kybernetické bezpečnosti pro režim vyšších povinností pro oblast organizačních opatření, včetně souvisejících obecně závazných právních předpisů.

V kapitole Rozsah plnění je vždy hovořeno o souboru samostatných dokumentů nicméně pokud je možné konkrétní dokument (politiku, metodiku, postup, šablonu atd.) nebo oblast řešit jako kapitolu nebo samostatnou část jiného dokumentu (například sloučit více příbuzných oblastí do jednoho dokumentu), dodavatel toto řešení upřednostní a navrhne. Samostatné dokumenty budou vznikat pouze tam, kde je to účelné z hlediska přehlednosti, auditovatelnosti a naplnění požadavků vyhlášky.

Obecná pravidla platná pro všechny dílčí části celkového díla (tedy pro všechny zde uvedené podkapitoly/paragrafy v části nazvané „Rozsah plnění“):

Dodavatel je tedy povinen:

- Provést průzkum existujících podmínek na OU.
    - Tento průzkum musí zohlednit tu skutečnost, že OU je veřejnou vysokou školou, jejíž vnitřní struktura je decentralizovaná (zde zejména existence fakult a ústavu jako provozních jednotek s funkční samostatností a dále existence orgánů OU i orgánů jednotlivých fakult) a jejíž jednotlivé orgány se ocitají také v postavení orgánu veřejné moci (zde typicky rozhodování o právech a povinnostech uchazečů o studium a studentů). Tento průzkum musí zahrnout všechna relevantní aktiva, zejména jednotlivé úseky (bloky, sady) informací, údajů a dat; dále personální a organizační zajištění; dále použité technologie a prostředky; dále nastavené procesy a postupy (zde zejména vnitřní legislativa, metodiky a politiky).
- Na základě tohoto provedeného průzkumu podat úplný a pravdivý popis existujících podmínek na OU. Tento podaný popis srovnat s požadavky právních předpisů s významem pro kyberbezpečnost.

- Těmito právními předpisy jsou jednak předpisy platné a účinné v době provádění díla (zde zejména zákon č. 264/2025 Sb.) a dále předpisy, které vycházejí ze zákona č. 264/2025 Sb. nebo s ním souvisejí, byť by třeba ještě nebyly vydány nebo by nebyly účinné v době provádění díla (zde zejména: vyhláška o regulovaných službách; dále vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností). V případě dosud nevydaných nebo dosud neúčinných předpisů Dodavatel použije to znění předpisů, které je nejaktuálnější (zde zejména znění schválené Vládou České republiky, nebo znění vydané Národním úřadem pro kybernetickou a informační bezpečnost). V případě pochybností o použití právního předpisu je Dodavatel povinen se písemně dotázat OU na upřesnění, a to před započetím prací na té dílčí části díla, která toto upřesnění vyžaduje.

- Na základě tohoto srovnání navrhnout jednoznačná a konkrétní opatření pro uvedení existujících podmínek na OU s požadavky právních předpisů s významem pro kyberbezpečnost. Navržená opatření by proto měla mít zejména podobu konkrétních politik, které bude OU moci aplikovat do svého specifického prostředí a které budou způsobilé pro přezkoumání případným budoucím auditem.
    - OU nemá zájem na tom, aby jednotlivými výstupy (tedy jednotlivými dílčími částmi celkového díla) byly obecné nebo teoretické komentáře či doporučení k právním předpisům. OU má naopak zájem na tom, aby tyto výstupy měly podobu konkrétních bezpečnostních politik použitelných v prostředí OU. OU má zejména zájem na tom, aby takové politiky obsahovaly jednoznačná vymezení pravidel, odpovědností a postupů pro danou konkrétní oblast bezpečnosti.
- Jednoznačně zhodnotit, zdali jednotlivé činnosti, funkce a role, které požadují relevantní právní předpisy, jsou na OU náležitě personálně obsazeny, zejména, zdali je na OU zřízena či ustavena (pracovní) pozice, funkce, či role požadovaná právními předpisy a zdali je tato (pracovní) pozice, funkce, či role obsazena dostatečným počtem osob. Součástí takového zhodnocení pak musí být konkrétní návrh nápravy případného nevhodného, nebo nedostatečného stavu.

Nepřítomnost nebo nedodání jednoznačných a konkrétních výstupů (zejména politik) jako dílčích částí celkového díla se považuje za podstatnou vadu díla.

Rozsah plnění

§ 4. Systém řízení bezpečnosti informací

Předpokládaný výstup je dokument Strategie kybernetické bezpečnosti informací (Strategie SŘBI OU), který bude minimálně:

a) Identifikovat všechny povinné oblasti (např. účel a význam, závazek vedení, identifikace regulovaných služeb, stanovení cílů, rozsahu SŘBI a jeho vyhodnocování) a přesně je přiřazovat k odpovídajícím paragrafům vyhlášky pro vyšší režim.

b) U každé oblasti stručně popíše účel a základní požadavek, přičemž jasně stanoví, pokud to bude naplnění požadavku vyžadovat, že detailní rozpracování bude provedeno v navazujících, samostatných dokumentech (např. opatřeních rektora, metodikách, plánech a obecně bezpečnostních dokumentací).

c) Dokument bude sloužit jako zastřešující rámec a strategická mapa pro naplnění všech organizačních povinností v oblasti SŘBI OU s odkazy do oblasti technických opatření, pokud to bude relevantní.

§ 5. Požadavky na vrcholné vedení

Dodavatel musí popsat klíčové povinnosti vrcholného vedení dle § 5 vyhlášky. Tyto povinnosti musí výslovně zohlednit při tvorbě Strategie řízení bezpečnosti informací Ostravské univerzity (SŘBI OU) kde budou jasně identifikovány a přiřazeny k odpovědným osobám nebo orgánům univerzity. Strategie SŘBI OU bude obsahovat kapitolu nebo samostatnou část věnovanou úloze a odpovědnostem vrcholného vedení v systému řízení bezpečnosti informací.

§ 6. Stanovení bezpečnostních rolí

Dodavatel musí popsat klíčové povinnosti vrcholného vedení dle § 6 vyhlášky. Tyto povinnosti, musí při zohlednit při tvorbě Strategie řízení bezpečnosti informací Ostravské univerzity (SŘBI OU), výslovně zohlednit a popsat klíčové povinnosti stanovení bezpečnostních rolí dle § 6 vyhlášky. Tyto povinnosti budou v dokumentu jasně identifikovány, přiřazeny konkrétním pracovním pozicím, funkcím, členům orgánů a orgánům OU a provázány s povinnostmi vrcholného vedení dle § 5. Strategie SŘBI OU bude obsahovat kapitolu nebo samostatnou část věnovanou bezpečnostním rolím, jejich pravomocem, odpovědnostem, požadavkům na kvalifikaci a zastupitelnost.

§ 7. Řízení bezpečnostní politiky a bezpečnostní dokumentace

Dodavatel na základě provedené analýzy současného stavu SŘBI na univerzitě a na základě Strategie SŘBI OU vytvoří a navrhne sadu samostatných bezpečnostních politik a navazující bezpečnostní dokumentace. Každý dokument bude samostatně

identifikovat konkrétní oblast, stanovovat pravidla (povinnosti), odpovědnosti a postupy, a bude odpovídat rozsahu a obsahu požadovanému vyhláškou pro konkrétní oblast.

Příkladová množina politik:

- Politika řízení dodavatelů, včetně návrhu povinných smluvních ustanovení
- Politika bezpečnosti lidských zdrojů
- Politika chování uživatelů, administrátorů a osob v bezpečnostních rolích
- Politika bezpečného používání mobilních zařízení
- Politika řízení změn
- Politika vývoje a provozu IS a DB
- Politika řízení přístupu
- Politika zvládání kybernetických bezpečnostních událostí a incidentů
- Politika řízení kontinuity činností
- Politika fyzické bezpečnosti
- Politika bezpečnosti komunikačních sítí (infrastruktury)
- Politika pro zaznamenávání událostí
- Politika nasazení, používání a údržby nástrojů pro detekci a vyhodnocování bezpečnostních událostí
- Politika řízení zranitelností a patch managementu
- Politika používání kryptografie
- Politika dlouhodobého ukládání, zálohování a obnovy po havárii

Příkladová množina bezpečnostní dokumentace a metodik:

- Plán provádění auditu kybernetické bezpečnosti
- Zpráva z auditu kybernetické bezpečnosti
- Zpráva z přezkoumání (vyhodnocení) SŘBI
- Prohlášení o aplikovatelnosti (viz § 9)
- Plán zvládání rizik
- Plán rozvoje bezpečnostního povědomí
- Metodika pro provedení analýzy dopadů
- Plány kontinuity činností (BCP)
- Plány obnovy (DRP) u vybraných podpůrných aktiv
- Evidence technických aktiv a autentizačních mechanismů

Dokumenty uvedené v příkladových množinách jsou minimálním výčtem samostatných dokumentů nebo samostatných kapitol v podobě komplexních dokumentů (viz. kapitola Zadání druhý odstavec).

§ 8. Řízení aktiv

Dodavatel vytvoří zcela konkrétní, auditovatelné dokumenty, které budou splňovat všechny povinnosti § 8. Dodavatel vytvoří minimálně:

a) Metodiku identifikace a hodnocení aktiv. Metodika bude popisovat postupy pro identifikaci, kategorizaci a hodnocení aktiv.

b) Registr reálných a konkrétních aktiv OU, který obsahuje seznam všech aktiv relevantních pro regulované služby. U každého aktiva navrhne strukturu metadat (např. název, typ, vlastník/garant, úroveň, klasifikace, vazby na další aktiva formou grafického schématu nebo tabulky vazeb). Podpůrná aktiva mohou být sdružena do logických množin.

c) Pravidla pro pravidelnou aktualizaci registru, pokud nebude zahrnuto v Metodice nebo v Strategii SŘBI OU jako explicitní kapitola.

d) Pravidla ochrany a používání aktiv.

Příkladová množina pravidel ochrany a používání aktiv (samostatné dokumenty nebo kapitoly):

- Přípustné způsoby používání aktiv
- Pravidla pro manipulaci s aktivy
- Pravidla pro klasifikaci informací (*vazba na již existující opatření rektora k ochraně dat v gesci prorektora pro výzkum a uměleckou činnost, pokud bude existovat*)
- Pravidla pro označování aktiv
- Pravidla správu výměnných médií
- Pravidla pro bezpečné elektronické sdílení a fyzické přenášení aktiv
- Pravidla pro likvidaci informací, dat a technických aktiv (včetně způsobu likvidace podle úrovně aktiva)

§ 9. Řízení rizik

Dodavatel vytvoří zcela konkrétní, auditovatelné dokumenty, které budou splňovat všechny povinnosti § 9. Dodavatel vytvoří minimálně:

a) Metodiku identifikace a hodnocení rizik. Metodika bude popisovat postupy pro identifikaci, kategorizaci a hodnocení rizik.

b) Analýza rizik.

c) Registr rizik, který obsahuje identifikátor, popis a vazbu na aktiva. Hodnocení dopadu, pravděpodobnosti a prioritu řešení.

d) Šablonu Zprávy o hodnocení rizik v rozsahu shrnutí identifikovaných rizik, vyhodnocení účinnosti stávajících opatření a doporučení pro nová opatření.

e) Prohlášení o aplikovatelnosti dle § 9 odst. 1 písm. f) Vyhlášky.

f) Plán zvládání rizik (příklad rozsahu Identifikátor rizika, popis opatření, odpovědná osoba, termín realizace, požadované zdroje (lidské, finanční, technické))

Registr rizik musí být propojen s Plánem zvládání rizik a Registrem aktiv.

§ 10. Řízení dodavatelů

Dodavatel vytvoří zcela konkrétní, auditovatelné dokumenty, které budou splňovat všechny povinnosti § 10. Dodavatel vytvoří minimálně:

a) Politiku řízení dodavatelů viz. Příkladová množina z § 7. Řízení bezpečnostní politiky a bezpečnostní dokumentace (např. povinnosti dodavatelů, proces seznamování dodavatelů s pravidly a požadavky univerzity a kritéria pro určení významného dodavatele)

b) Registr dodavatelů s identifikací významných dodavatelů.

c) Návrh základní množiny šablon pro prokazatelné informování významného dodavatele.

d) Návrh Plánu a záznamu z pravidelného přezkumu plnění smluv.

§ 11. Bezpečnost lidských zdrojů

Dodavatel vytvoří zcela konkrétní, auditovatelné dokumenty, které budou splňovat všechny povinnosti § 11. Výstupy musí být strukturovány podle cílových skupin (vrcholné vedení, uživatelé zaměstnanci a studenti, dodavatelé) a zahrnovat:

a) Plán rozvoje bezpečnostního povědomí. Navrhne konkrétní harmonogram školení pro jednotlivé množiny uživatelů viz. b).

b) Základní školící materiály (vzdělávací text + návrh testu) pro

   - Uživatele **vrcholné vedení** ve formě desatera odpovědného vedení v oblasti kybernetické bezpečnosti (např. podpora bezpečnostní kultury, schvalování politik, osobní příklad, povinnost školení, reakce na incidenty) se zaměřením na povinnosti a řízení SŘBI, včetně zdůraznění odpovědnosti.
   - Uživatele **zaměstnanci** ve formě desatera bezpečného uživatele (např. silná hesla, nikdy nesdělovat přístupové údaje, hlášení podezřelých e-mailů, bezpečné zacházení s daty, zamykání počítače, zákaz instalace neověřeného softwaru, pravidla pro práci z domova a jiné).
   - Uživatele **studenti** ve formě desatero bezpečného studenta (např. ochrana vlastních účtů, zásady bezpečné komunikace, jak poznat podvodný e-mail, pravidla pro sdílení studijních materiálů, respektování autorských práv).
   - Uživatele **dodavatelé** taktéž ve formě určitého desatera bezpečného dodavatele (důraz na pravidla přístupu, nakládání s daty, povinnosti při incidentu, ochrana před malwarem, bezpečná práce na dálku, dodržení smluvních bezpečnostních požadavků).

§ 12. Řízení změn

Dodavatel vytvoří zcela konkrétní, auditovatelné dokumenty, které budou splňovat všechny povinnosti § 12. Dodavatele navrhne minimálně:

a) Politiku řízení změn viz. Příkladová množina z § 7. Řízení bezpečnostní politiky a bezpečnostní dokumentace definující pravidla pro identifikaci, klasifikaci (běžná/významná) změn a schvalování změn.

   - Kritéria pro určení "významné změny" (např. dopad na dostupnost služby, riziko úniku dat).
   - Role a odpovědnosti (schvalovatelé, implementátoři).

b) Metodiku řízení významných změn ve formě návrhu procesu řízení změn (kroky: identifikace změny → posouzení rizik → schválení → implementace → testování → roll-back plán) včetně návrhu šablon pro dokumentaci každého kroku (např. formulář pro posouzení rizik).

Propojení s Registrem rizik (§9) a Bezpečnostní politikou (§7) .

§ 13. Akvizice, vývoj a údržba

Dodavatel vytvoří zcela konkrétní, auditovatelné dokumenty, které budou splňovat všechny povinnosti § 13.

Dodavatele navrhne Metodiku vývoje, která popíše základní proces vývoje informačních systémů a aplikací. Stanovuje povinnost identifikovat a hodnotit rizika spojená s vývojem (§ 12 Řízení změn). Ukládá povinnost oddělit vývojové, testovací a produkční prostředí a chránit data v těchto prostředích. Stanovuje základní bezpečnostní požadavky na vývoj (např. autentizace, bezpečná hesla, kryptografie – odkaz na § 20 a § 26 Technických opatření). Ukládá povinnost dokumentovat všechny významné změny a provádět jejich schvalování.

§ 14. Řízení přístupu

Dodavatel vytvoří zcela konkrétní, auditovatelné dokumenty, které budou splňovat všechny povinnosti § 14. Dodavatel navrhne minimálně:

a) Politiku řízení přístupu a správy identit viz. Příkladová množina z § 7. Řízení bezpečnostní politiky a bezpečnostní dokumentace definující pravidla pro přidělování, změnu a odebrání přístupových práv, pravidla pro minimální nutná oprávnění a pravidla pro oddělení uživatelských a administrátorských účtů.

b) Metodiku správy přístupových práv a oprávnění popisující postupy pro přidělování, změnu a odebrání práv včetně evidence. Definuje povinnost pravidelného přezkumu přístupových práv (např. pololetní/roční revize) a postupy při změně pozice, pracoviště a ukončení pracovního poměru či smluvního vztahu.

§ 15. Zvládání kybernetických bezpečnostních událostí a incidentů

Dodavatel vytvoří zcela konkrétní, auditovatelné dokumenty, které budou splňovat všechny povinnosti § 15. Dodavatel navrhne minimálně:

a) Politiku zvládání událostí a incidentů viz. Příkladová množina z § 7. Řízení bezpečnostní politiky a bezpečnostní dokumentace definující pravidla a odpovědnosti pro detekci, zaznamenávání, vyhodnocování a zvládání událostí a incidentů. Postupy pro oznamování, eskalaci, analýzu a řešení incidentů a návrh pravidel pro sběr a uchování důkazních podkladů.

b) Metodiku detekce, vyhodnocování a klasifikace událostí určující postupy pro detekci a vyhodnocení událostí, včetně rozhodovacího procesu, kdy je událost klasifikována jako incident a musí se hlásit na NÚKIB via. Portal NÚKIB. Zdůraznit vazby na nástroje a postupy podle § 22 a § 24.

c) Šablonu Incident Response Plan pro vybranou regulovanou službu, resp. primární aktivum v podobě návrhu praktického plánu s kroky pro zvládání incidentů, tj. od oznámení, eskalaci, koordinaci, komunikaci, technických kroků až po ukončení incidentu. Role a kontakty odpovědných osob.

d) Šablonu Zprávy o vyhodnocení incidentů definující povinnost analýzy příčin, přijatých opatření, vyhodnocení účinnosti a návrhy na aktualizaci politik a procesů, aby se zabránilo opakování incidentu.

§ 16. Řízení kontinuity činností

Dodavatel vytvoří zcela konkrétní, auditovatelné dokumenty, které budou splňovat všechny povinnosti § 16. Dodavatel navrhne minimálně:

a) Metodiku pro provedení analýzy dopadu popisující postup identifikace a vyhodnocení dopadů incidentů na provoz univerzity a regulované služby. Vazbu na hodnocení rizik (§ 9). Kritéria pro stanovení minimální úrovně regulovaných služeb, doby obnovení chodu a časového období obnovení dat ze záloh, aby byl zajištěn chod univerzity, výzkumných projektů, regulovaných služeb.

b) Plány kontinuity činností (BCP) a plány obnovy (DRP) pro klíčovou regulovanou službu, kterou určí Zadavatel. Postupy pro reakci na incident, obnovu provozu a dat. Konkrétní kontakty, odpovědnosti, harmonogramy obnovy. Návrhy protokolů z pravidelného testování plánů.

§ 17. Provádění auditu kybernetické bezpečnosti

Dodavatel vytvoří zcela konkrétní, auditovatelné dokumenty, které budou splňovat všechny povinnosti § 17. Dodavatel navrhne minimálně:

a) Plán provádění auditu kybernetické bezpečnosti popisující mimo jiné i účel auditu, jeho význam pro univerzitu, návaznost na vyhlášku a další interní předpisy viz. Příkladová množina bezpečnostní dokumentace a metodik z § 7. Řízení bezpečnostní politiky a bezpečnostní dokumentace

Shrnutí

1. **Struktura a členění dokumentace**
   Připravit konkrétní návrh struktury výsledné dokumentace formou tabulky (např. formou rozcestníku), která jasně ukáže, které oblasti budou řešeny jako samostatné dokumenty a které jako kapitoly v rámci větších celků. (příklad struktury: název dokumentu/kapitoly, oblast pokrytí, vazbu na paragraf vyhlášky, odpovědnou osobu, návaznosti na další dokumenty, a typ výstupu (politika, metodika, plán, šablona atd.))

2. **Vazby na konkrétní paragrafy a legislativní požadavky**
   U každé oblasti explicitně uvádět, které konkrétní paragrafy vyhlášky a zákona daný dokument/kapitola naplňuje. Tím se zvýší auditovatelnost a srozumitelnost pro kontrolní orgány.

3. **Vnitřní provázanost dokumentace**
   Při návrhu dokumentací vždy dodržovat vzájemnou provázanost, tj. jak na sebe jednotlivé politiky, metodiky a plány navazují, jaké jsou mezi nimi vazby (např. plán zvládání rizik musí být propojen s registrem aktiv i rizik, plán kontinuity s analýzou dopadů atd.)

4. **Důraz na pravidelnou aktualizaci a revize**
   U každé oblasti stanovit pravidla pro pravidelnou revizi a aktualizaci dokumentace, včetně odpovědných osob a termínů.

5. **Analýza SŘBI OU**
   Zadavatel má k dispozici množinu bezpečnostní dokumentace, včetně interních směrnic, které upravují vybrané procesy v SŘBI. Tyto dokumenty budou sloužit jako podklad pro realizaci Předmětu plnění. Předmětem plnění není revize stávající dokumentace, politik, neformálních metodik nebo řídících opatření.

Harmonogram (nový)

Dílčí části celkového díla (tedy jednotlivé zde uvedené podkapitoly/paragrafy v části nazvané „Rozsah plnění“)	Mezní termín pro provedení (dokončení a předání) konkrétní dílčí části celkového díla stanovený počtem kalendářních dnů po dni účinnosti smlouvy
§ 4 Systém řízení bezpečnosti informací	**30**
§ 5 Požadavky na vrcholné vedení	**90**
§ 6 Stanovení bezpečnostních rolí	**90**
§ 7 Řízení bezpečnostní politiky a bezpečnostní dokumentace	**330**
§ 8 Řízení aktiv	**90**
§ 9 Řízení rizik	**120**
§ 10 Řízení dodavatelů	**150**
§ 11 Bezpečnost lidských zdrojů	**180**
§ 12 Řízení změn	**210**
§ 13 Akvizice, vývoj a údržba	**240**
§ 14 Řízení přístupu	**240**
§ 15 Zvládání kybernetických bezpečnostních událostí a incidentů	**210**
§ 16 Řízení kontinuity činností	**300**
§ 17 Provádění auditu kybernetické bezpečnosti	**330**

Příklad: Lhůta pro splnění kapitoly § 8 Řízení aktiv je 90 dnů ode dne účinnosti smlouvy. Lhůta pro splnění kapitoly § 16 Řízení kontinuity činností je 300 dnů ode dne účinnosti smlouvy.