# 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](#_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

### Systém řízení bezpečnosti informací

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

1. 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.
2. 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).
3. 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.

### 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](#_Systém_řízení_bezpečnosti) bude obsahovat kapitolu nebo samostatnou část věnovanou úloze a odpovědnostem vrcholného vedení v systému řízení bezpečnosti informací.

### 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](#_Systém_řízení_bezpečnosti) bude obsahovat kapitolu nebo samostatnou část věnovanou bezpečnostním rolím, jejich pravomocem, odpovědnostem, požadavkům na kvalifikaci a zastupitelnost.

### 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](#_Zadání) druhý odstavec).

### Řízení aktiv

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

1. Metodiku identifikace a hodnocení aktiv. Metodika bude popisovat postupy pro identifikaci, kategorizaci a hodnocení aktiv.
2. 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.
3. Pravidla pro pravidelnou aktualizaci registru, pokud nebude zahrnuto v Metodice nebo v Strategii SŘBI OU jako explicitní kapitola.
4. 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)

### Řízení rizik

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

1. Metodiku identifikace a hodnocení rizik. Metodika bude popisovat postupy pro identifikaci, kategorizaci a hodnocení rizik.
2. Analýza rizik.
3. Registr rizik, který obsahuje identifikátor, popis a vazbu na aktiva. Hodnocení dopadu, pravděpodobnosti a prioritu řešení.
4. Šablonu Zprávy o hodnocení rizik v rozsahu shrnutí identifikovaných rizik, vyhodnocení účinnosti stávajících opatření a doporučení pro nová opatření.
5. Prohlášení o aplikovatelnosti dle § 9 odst. 1 písm. f) Vyhlášky.
6. 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.

### Řízení dodavatelů

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

1. Politiku řízení dodavatelů viz. [Příkladová množina](#_Příkladová_množina_politik:) z [§ 7. Řízení bezpečnostní politiky a bezpečnostní dokumentace](#_Řízení_bezpečnostní_politiky) (např. povinnosti dodavatelů, proces seznamování dodavatelů s pravidly a požadavky univerzity a kritéria pro určení významného dodavatele)
2. Registr dodavatelů s identifikací významných dodavatelů.
3. Návrh základní množiny šablon pro prokazatelné informování významného dodavatele.
4. Návrh Plánu a záznamu z pravidelného přezkumu plnění smluv.

### 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:

1. Plán rozvoje bezpečnostního povědomí. Navrhne konkrétní harmonogram školení pro jednotlivé množiny uživatelů viz. b).
2. 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).

### Řízení změn

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

1. Politiku řízení změn viz. [Příkladová množina](#_Příkladová_množina_politik:) z [§ 7. Řízení bezpečnostní politiky a bezpečnostní dokumentace](#_Řízení_bezpečnostní_politiky) 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).
2. 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)](#_Řízení_rizik) a [Bezpečnostní politikou (§7)](#_Řízení_bezpečnostní_politiky) .

### 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](#_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.

### Řízení přístupu

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

1. Politiku řízení přístupu a správy identit viz. [Příkladová množina](#_Příkladová_množina_politik:) z [§ 7. Řízení bezpečnostní politiky a bezpečnostní dokumentace](#_Řízení_bezpečnostní_politiky) definující pravidla pro přidělování, změnu a odebrání přístupových práv, pravidla pro minimální nutná oprávnění a pravidla pro oddělení uživatelských a administrátorských účtů.
2. 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.

### Zvládání kybernetických bezpečnostních událostí a incidentů

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

1. Politiku zvládání událostí a incidentů viz. [Příkladová množina](#_Příkladová_množina_politik:) z [§ 7. Řízení bezpečnostní politiky a bezpečnostní dokumentace](#_Řízení_bezpečnostní_politiky) 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.
2. 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.
3. 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.
4. 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.

### Řízení kontinuity činností

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

1. Metodiku pro provedení analýzy dopadu popisující postup identifikace a vyhodnocení dopadů incidentů na provoz univerzity a regulované služby. Vazbu na [hodnocení rizik (§ 9).](#_Řízení_rizik) 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.
2. 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.

### Provádění auditu kybernetické bezpečnosti

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

1. 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](#_Příkladová_množina_politik:) z [§ 7. Řízení bezpečnostní politiky a bezpečnostní dokumentace](#_Řízení_bezpečnostní_politiky)

# 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.))

1. **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.

1. **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.)

1. **Důraz na pravidelnou aktualizaci a revize**

U každé oblasti stanovit pravidla pro pravidelnou revizi a aktualizaci dokumentace, včetně odpovědných osob a termínů.

1. **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.