Univerzita Palackého
v Olomouci

Genius loci ...

Univerzita Palackého v Olomouci je **subjektem podléhajícím regulaci zákona 181/2014 Sb., zákon o kybernetické bezpečnosti**. Univerzita Palackého v Olomouci tak v souladu se svou zákonnou povinností vyhodnotila, že je správcem několika tzv. významných informačních systémů (když významným informačním systémem je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci).

Plněním předmětu objednávky (dodávky zboží nebo služeb) ze strany Vaší společnosti dochází k aktivitě související s funkčností technických a programových prostředků tvořících daný informační nebo komunikační systém.

UP jakožto správce/provozovatel významných informačních systémů tímto Vaši společnost souladně s § 8 vyhlášky č. 82/2018 Sb., vyhláška o kybernetické bezpečnosti, informuje o následujícím:

Identifikace správce/provozovatele významného informačního systému	Univerzita Palackého v Olomouci
Dotčený významný informační systém	Spisová služba ERMS ERP SAP STAG

Společně s informací výše je UP zároveň povinna **stanovit pravidla pro dodavatele**, která zohledňují požadavky systému řízení bezpečnosti informací na UP, **a informovat** Vaši společnost jakožto dodavatele **o obsahu těchto pravidel**.

Vzorová bezpečnostní pravidla pro významné dodavatele jsou přiložena jakožto příloha tohoto listu; zdvořile Vás žádáme o seznámení s těmito pravidly a jejich maximální možnou implementaci.

Příloha: Bezpečnostní pravidla pro významné dodavatele

Příloha: Bezpečnostní pravidla pro významné dodavatele

Cílem těchto bezpečnostních pravidel je snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránící Aktiva Univerzity Palackého v Olomouci (dále jen „**objednatel**“), ke kterým mají přístup Dodavatelé dle ustanovení § 4 odst. 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění (dále jen „**Zákon**“), ve spojení v přílohou č. 7 k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „**Vyhláška**“).

Základní odpovědnosti Dodavatele

Dodavatel řešení:

a. Je povinen postupovat v souladu s platnými právními předpisy, zejména pak v souladu s požadavky vyplývajícími pro objednatele, jakožto správce a provozovatele Významného informačního systému, ze Zákona a Vyhlášky a reflektovat případné novely uvedených právních předpisů či novou právní úpravu;

b. Odpovídá za své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost Objednatel, zabránilo bezpečnostním incidentům a krizovým situacím;

c. Odpovídá za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti.

d. Je povinen zajistit, aby předmět plnění nebyl nevyhovující z hlediska informační bezpečnosti, přičemž za nevyhovující je považováno jakékoli plnění, které obsahuje technologie/klíčové prvky, vůči jejichž výrobcům příslušný správní orgán vydal opatření v souladu se Zákonem, a které dle analýzy rizik představují vysoké riziko;

e. Je povinen provádět analýzu a hodnocení rizik informační infrastruktury, která je součástí předmětu Smlouvy (dodávaného řešení) a na základě výsledků navrhovat a předkládat Objednatel ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik;

f. Je povinen zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost během poskytování plnění pro Objednatele;

g. Ručí za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s Objednatelem.

Ochrana Aktiv

1. Dodavatel se před vlastním **přístupem** k datům a informacím Objednatele musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků Objednatele zavázat Dodavatele a nezpřístupnit data a informace Dodavateli dříve, než dojde k jeho závazku mlčenlivosti (tj. podpisu NDA – Non Disclosure Agreement či CA – Confidentiality Agreement).

Řízení přístupu k ICT/IS

1. Přihlášení Dodavatele do sítě Objednatele musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci.

2. Dodavatel se zavazuje, že před připojením koncového zařízení, mobilní koncového zařízení nebo aktivního síťového prvku jako síťové switche, WiFi access pointy, routery či huby do počítačové sítě zažádá o schválení připojení kontaktní osobu na straně Objednatele.
3. Dodavatel se zavazuje, že vzdálený přístup do systému Objednatele bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.
4. Dodavatel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku.
5. Dodavatel se zavazuje, že nebude instalovat a používat zejména typy nástrojů Keylogger, Sniffer, Analyzátor zranitelností a Port Scanner, Backdoor, rootkit a trojský kůň nebo jinou podobu malware.
6. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednatele, kteří přistupují do interní sítě nebo informačního systému Objednatele, měli v externím zařízení typu notebook/počítač aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.
7. Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Dodavatele nebo Poddodavatele.
8. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Dodavatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu.

Kontrola a Audit dodavatele

1. Dodavatel se zavazuje poskytnout Objednatele veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající z těchto pravidel, jakož i ze Zákona a Vyhlášky, a za tímto účelem se zavazuje umožnit Objednatele provedení kontrol, včetně auditů prováděných Objednatele či auditorem, kterého Objednatele k auditu pověří, a poskytne k těmto kontrolám a auditům veškerou potřebnou součinnost.
2. Dodavatel je povinen Objednatele zpřístupnit veškerou potřebnou dokumentaci pro účely kontroly či auditu, zejména výčet technických a organizačních opatření.
3. Dodavatel má povinnost určit svého zástupce (případně své zástupce), který bude po dobu provádění kontroly či auditu přítomen.
4. Dodavatel je dále povinen umožnit provedení kontroly či auditu i ze strany dozorových orgánů (např. Národnímu úřadu pro kybernetickou a informační bezpečnost)
5. Dodavatel se zavazuje umožnit Objednateli provést po vzájemné dohodě v rozsahu předmětu plnění testy dostupnosti, důvěrnosti a integrity dat, informací a jiných zdrojů Dodavatele, které jsou využívány k poskytování předmětu plnění, a poskytnout potřebnou součinnost;
6. Dodavatel se zavazuje zajistit bezodkladné odstranění zjištěných nedostatků a nesouladu s těmito Bezpečnostními požadavky.

Poddodavatelé

1. Dodavatel nezapojí do poskytování plnění dle této Smlouvy žádného dalšího Poddodavatele bez předchozího konkrétního nebo obecného povolení Objednatele.
2. Dodavatel je povinen předat Objednatele kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení.
3. Dodavatel má povinnost zajistit, že Poddodavatel bude v souladu s požadavky, které Objednatele ukládá na základě těchto Bezpečnostních pravidel Dodavateli.

4. Dodavatel odpovídá za to, že jeho Poddodavatelé nebudou jednat v rozporu s bezpečnostními opatřeními vyplývajícími z těchto Bezpečnostních pravidel; v případě, že dojde k nedodržení těchto požadavků ze strany Poddodavatele Dodavatele, považuje se každé takové nedodržení požadavků za porušení povinnosti Dodavatele dle Smlouvy.
5. Využití třetí osoby k plnění předmětu smlouvy nebo její části nezbavuje Dodavatele odpovědnosti za případnou škodu způsobenou Objednateli.

Řízení změn

1. Dodavatel se zavazuje určovat významné změny, za které se považují změny, které mají nebo mohou mít vliv na kybernetickou bezpečnost a představují vysoké riziko. Dodavatel je povinen o těchto významných změnách předem informovat Objednatele.
2. U významných změn se Dodavatel zavazuje zejména:
   i) provádět analýzu rizik;
   ii) přijímat opatření za účelem snížení negativních dopadů těchto změn, včetně případného penetračního testování a testování zranitelnosti;
   iii) dokumentovat jejich řízení;
   iv) aktualizovat specifickou bezpečnostní politiku pro danou v oblast;
   v) zajistit možnost navrácení do původního stavu.
3. V případě realizace penetračního testování nebo testování zranitelnosti řešení poskytne Dodavatel Objednateli veškerou potřebnou součinnost. Dodavatel je povinen přijmout dodatečná, účinná nápravná opatření k odstranění zranitelností, které byly zjištěny v průběhu penetračního testování.

Řízení bezpečnostních rizik

1. Dodavatel je povinen alespoň 1x ročně provádět vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. O výsledku hodnocení rizik Dodavatel Objednateli předloží Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:
   vi) vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok, včetně vyhodnocení souladu s těmito Bezpečnostními požadavky
   vii) identifikaci a hodnocení rizik s vazbou na předmět plnění,
   viii) realizovaná bezpečnostní opatření,
   ix) nepokrytá bezpečnostní rizika a návrh opatření,
   x) vyhodnocení bezpečnostních událostí a incidentů.

Monitorování činností

1. Dodavatel bere na vědomí, že veškerá jeho aktivita realizovaná v informačních systémech, může být Objednatelem průběžně a pravidelně monitorována.
2. Předmět plnění musí poskytovat auditní záznamy (logy) o činnostech v něm provedených, v rozsahu stanoveném Vyhláškou, které umožní jednoznačně určit uživatele, čas a provedenu činnost.
3. Dodavatel se zavazuje, že umožní přístup k auditním údajům (systémové a aplikační logy) v takové podobě a formátu, který je možné dále zpracovávat v rámci systému nástrojů SIEM (Security Information Event Management) a jejich archivaci.

Zvládání kybernetických bezpečnostních incidentů

1. Dodavatel se zavazuje, že bude hlásit všechny nestandardní situace, bezpečnostní slabiny, kybernetické bezpečnostní události a incidenty včetně případů porušení zabezpečení osobních údajů bez zbytečného odkladu po jejich detekci Objednateli.
2. Hlášení provádí Dodavatel telefonicky na linku 602/376365 a písemně na helpdesk@upol.cz. Součástí oznámení musí být popis povahy případu.
3. Pokud dojde ke kybernetické bezpečnostní události nebo ke kybernetickému bezpečnostnímu incidentu a následnému zvládání a vyhodnocování kybernetického bezpečnostního incidentu na bezpečnostní incident na straně Objednatele, poskytne Dodavatel požadovanou součinnost např.: poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, HW typ, sériové číslo případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení, k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná Objednatelem).
4. Dodavatel má povinnost provést analýzu příčin kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.
5. Dodavatel má povinnost uchovávat informace o kybernetických bezpečnostních událostech a incidentech pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.

Informační povinnost dodavatele

1. Dodavatel má povinnost bez zbytečného odkladu informovat Objednatele o významné změně ovládání Dodavatele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví základních aktiv, jakož i změně v oprávnění Dodavatele nakládat s aktivy, které jsou využívány k plnění předmětu Smlouvy.
2. Dodavatel má povinnost informovat Objednatele o způsobu řízení rizik, jakož i o zbytkových rizicích souvisejících s plněním předmětu Smlouvy.

Výměna informací

1. Dodavatel se zavazuje, že veškerý přenos dat a informací musí být dostatečně zabezpečen pomocí aktuálně odolných kryptografických algoritmů a kryptografických klíčů.
2. Dodavatel se zavazuje, že on-line transakce realizované prostřednictvím webových technologií budou chráněny SSL certifikáty.

Řízení kontinuity činností

1. Dodavatel zavazuje zejména:
   xi) určit minimální úroveň poskytovaných služeb přijatelnou z hlediska zajištění kontinutity poskytovaných činností;
   xii) určit dobu obnovení chodu, během které bude po bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb dle písm. b);
   xiii) určit časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání;

xiv) vypracovat, aktualizovat a pravidelně testovat plány kontinuity činnosti a havarijní plány související s poskytováním předmětu plnění.

2. Objednatel má oprávnění zapojit Dodavatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Dodavatele do plánu kontinuity činností včetně jeho testování, který souvisí s VIS a souvisejících služeb a/nebo zahrnutí Dodavatele do havarijního plánu Objednatele.
3. Dodavatel předloží Objednateli metodiku zálohování a obnovy dat ve formě zálohovacího plánu, testovacího scénáře obnovy dat, systému evidence, zajištění integrity a autenticity zálohovacího média. Záloha jako taková musí být šifrována.

Likvidace dat

1. Pokud v rámci plnění předmětu Smlouvy má Dodavatel povinnost k mazání dat a k likvidaci technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií, postupuje vždy v souladu s pravidly pro mazání dat a v souladu se způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií na základě tabulky č.1. Přičemž, pokud není určena klasifikace informace, bude použit způsob likvidace pro důležitost aktiva kritickou.

Povinnosti při ukončení smlouvy

1. Dodavatel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s Objednateli a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, podporou a rozvojem předmětu Smlouvy na Objednatele a/nebo nového dodavatele, ke kterému dojde po skončení účinnosti této Smlouvy, a to vše dle pokynů Objednatele (dále jen „**Ukončení smlouvy**“).
2. Dodavatel se zavazuje za tímto účelem vypracovat a nejpozději spolu s provozní dokumentací ke každému předávanému dílčímu plnění předat Objednateli dokumentaci, která bude stanovovat postup při Ukončení smlouvy (dále jen „**Plán**“). Dodavatel se zavazuje Plán po dobu trvání této Smlouvy průběžně aktualizovat a Objednatele vždy při změně jakékoliv skutečnosti uvedené v Plánu předat aktualizovanou verzi Plánu zohledňující tuto změnu.
3. Dodavatel je povinen poskytnout plnění nezbytná k realizaci tohoto Plánu za přiměřeného použití vhodných ustanovení této Smlouvy. Závazek dle tohoto ustanovení platí i po ukončení této Smlouvy.
4. Strany se dohodly, že cena za vypracování Plánu a poskytnutí plnění nezbytného k realizaci Plánu je součástí ceny dle této Smlouvy.

Tato Bezpečnostní pravidla jsou v souladu s platnými právními předpisy České republiky. Pokud se jakékoli ustanovení těchto Bezpečnostních pravidel stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních ustanovení těchto Bezpečnostních pravidel a rovněž Smlouvy. Strany se zavazují nahradit neplatné nebo nevymahatelné ustanovení novým ustanovením, jehož znění bude odpovídat úmyslu vyjádřenému původním ustanovením a těchto Bezpečnostních pravidel jako celkem.

Tabulka č. 1

<table>
<tr><th></th><th colspan="4">Přípustný způsob likvidace podle úrovně důležitosti aktiva</th></tr>
<tr><th>Nosič informace</th><th>1. Nízká</th><th>2. Střední</th><th>3. Vysoká</th><th>4. Kritická</th></tr>
<tr><td>Informace na lidsky čitelném nosiči (tištěné dokumenty, poznámky a podobně)</td><td>Odstranění: Vyhození do odpadu.</td><td>Přepsání: Začernění.</td><td colspan="2" rowspan="2">Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.</td></tr>
<tr><td></td><td>Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje.</td></tr>
<tr><td>Mobilní zařízení (mobilní telefony, tablety)</td><td>Odstranění: Vymazání informací, reset zařízení do továrního nastavení.</td><td>Přepsání: Pro zařízení s šifrovaným úložištěm - odstranění informací a reset do továrního nastavení.</td><td colspan="2" rowspan="3">Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.</td></tr>
<tr><td>Síťová zařízení (router, switch, modem a podobně)</td><td rowspan="2">Odstranění: Vymazání informací, reset do továrního nastavení.</td><td rowspan="2">Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně.).</td></tr>
<tr><td>Kancelářské vybavení (scanery, tiskárny, fax)</td></tr>
<tr><td>Magnetická média (magnetické pásky, disky, HDD [Hard Disk Drive])</td><td rowspan="3">Odstranění: Smazání dat na úrovni souborového systému.</td><td rowspan="2">Přepsání: Přepsání dat. V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů</td><td colspan="2" rowspan="2">Fyzická likvidace: Zničení nosiče informací.</td></tr>
<tr><td>Optická média (CD, DVD, HD-DVD, BLU-RAY)</td></tr>
<tr><td>Elektronická média (flash paměti)</td><td>Fyzická likvidace.</td></tr>
<tr><td rowspan="2">Outsourcing a cloud</td><td colspan="4">Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním.</td></tr>
<tr><td>Odstranění: Odstranění všech souborů včetně předchozích verzí.</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických</td><td>Přepsání/fyzická likvidace: Použit způsob viz úroveň “3. Vysoká” nebo použita dedikovaná paměťová kapacita úložiště. Při</td></tr>
</table>

		likvidace kryptografických klíčů. Alternativně v případě dedikovaného paměťového média je možné data po ukončení služby přepsat.	klíčů uložených v certifikovaném hardware security modulu (HSM) řízená zákazníkem (například podle standardu FIPS 140-2 Level 2). Při ukončení služby bude zlikvidován vrchní přístupový klíč a data jsou přepsána.	ukončení služby provedena celková sanitizace všech použitých paměťových médií podle výše uvedených řádků pro úroveň kritická.