Cílem těchto bezpečnostních pravidel je snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránící Aktiva BMT Medical Technology s.r.o. (dále jen „**BMT**“), 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**“).

1 Základní odpovědnosti dodavatele

Dodavatel řešení:

1. Je povinen postupovat v souladu s platnými a účinnými právními předpisy, zejména pak v souladu s požadavky vyplývajícími pro BMT, jakožto správce a provozovatele Významného informačního systému, ze Zákona a Vyhlášky a reflektovat případné novely uvedených právních předpisů či novou právní úpravu;
2. odpovídá za své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost BMT, zabránilo bezpečnostním incidentům a krizovým situacím;
3. odpovídá za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti.
4. 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;
5. je povinen provádět analýzu a hodnocení rizik informační infrastruktury, která je součástí předmětu Smlouvy (dodávaného řešení) a na základě výsledků navrhovat a předkládat BMT ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik;
6. je povinen zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost během poskytování plnění pro BMT;
7. odpovídá za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s BMT.

2 Ochrana aktiv

Dodavatel se před vlastním **přístupem** k datům a informacím BMT musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků BMT 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).

3 Řízení přístupu k ICT/IS

1. Přihlášení dodavatele do sítě BMT musí podléhat kontrole přístupu na základě smluvního vztahu - 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 BMT.
3. Dodavatel se zavazuje, že vzdálený přístup do systému BMT 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 BMT, které přistupují do interní sítě nebo informačního systému BMT, měly 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 subdodavatele.

4 Audit dodavatele

1. Dodavatel se zavazuje poskytnout BMT 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 BMT provedení kontrol, včetně auditů prováděných BMT či auditorem, kterého BMT k auditu pověří, a poskytne k těmto kontrolám a auditům veškerou potřebnou součinnost.
2. Dodavatel je povinen BMT 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.

5 Subdodavatelé

1. Dodavatel nezapojí do poskytování plnění žádného dalšího subdodavatele bez předchozího konkrétního nebo obecného povolení BMT.
2. Dodavatel je povinen předat BMT kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení.
3. Dodavatel odpovídá za to, že jeho subdodavatelé nebudou jednat v rozporu s bezpečnostními opatřeními vyplývajícími z těchto Bezpečnostních pravidel; v případě, že dojde k nedodržení těchto požadavků ze strany subdodavatele dodavatele, považuje se každé takové nedodržení požadavků za porušení povinnosti dodavatele.

6 Řízení změn

1. BMT v rámci řízení změn v systému řízení kybernetické bezpečnosti přezkoumává možné dopady změn a určuje významné změny dle Vyhlášky.
2. Dodavatel se zavazuje poskytnout BMT veškerou nezbytnou součinnost při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.
3. V případě realizace penetračního testování nebo testování zranitelnosti řešení poskytne dodavatel BMT veškerou potřebnou součinnost. Dodavatel je povinen přijmout dodatečná, účinná nápravná opatření k odstranění zranitelností, které byly zjištěny v průběhu penetračního testování.

7 Řízení bezpečnostních rizik

Dodavatel je povinen pravidelně provádět také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených dodavatelem, na žádost BMT. O výsledku kontroly podá dodavatel BMT bez zbytečného odkladu písemnou kontrolní zprávu.

8 Monitorování činností

1. Dodavatel bere na vědomí, že veškerá jeho aktivita realizovaná v informačních systémech, může být BMT 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.

9 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 neprodleně po jejich detekci BMT.
2. Hlášení provádí dodavatel emailem na security@bmt.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 BMT, 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 BMT).
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.

10 Informační povinnost dodavatele

1. Dodavatel má povinnost bez zbytečného odkladu informovat BMT 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 BMT o způsobu řízení rizik, jakož i o zbytkových rizicích souvisejících s plněním předmětu Smlouvy.

11 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.

12 Řízení kontinuity činností

1. BMT má oprávnění zapojit Dodavatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí dodavatele do plánu kontinuity činností, který souvisí s VIS a souvisejících služeb a/nebo zahrnutí dodavatele do havarijního plánu BMT.
2. Dodavatel předloží BMT 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.

13 Likvidace dat

Pokud v rámci plnění předmětu Smlouvy má dodavatel povinnost k mazání dat a k likvidaci technických nosičů, 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.

14 Povinnosti při ukončení smlouvy

1. Dodavatel se zavazuje poskytnout BMT veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s BMT a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s

provozem, podporou a rozvojem předmětu Smlouvy na BMT a/nebo nového dodavatele, ke kterému dojde po skončení účinnosti této Smlouvy, a to vše dle pokynů BMT (dále jen „**Ukončení smlouvy**“).

2. Dodavatel se zavazuje za tímto účelem vypracovat a nejpozději spolu s provozní dokumentací ke každému předávanému dílčímu plnění předat BMT dokumentaci, která bude stanovovat postup při Ukončení smlouvy (dále jen „**Plán**“). Dodavatel se zavazuje Plán po dobu trvání této Smlouvy průběžně aktualizovat a BMT 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 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 celku.