# DOTAZNÍK PRO ZJIŠTĚNÍ KYBERNETICKÝCH RIZIK

**V případě, kdy ve Vaší Společnosti dojde ke ztrátě, úniku či zneužití dat (dále jen „incident“), považovaných za osobní údaje dle zvláštního právního předpisu (např. poskytování zdravotních služeb; poskytování komunikačních a telekomunikačních služeb; dodávky a distribuce elektrické energie, plynu, vody, atd.; poskytování bankovních a platebních služeb; pojišťovací služby, zprostředkování pojišťovacích služeb aj.), budete čelit vyšetřování tohoto incidentu ze strany státních orgánů (Policie ČR, ÚOOÚ, NÚKIB . . . . ), Vaší profesní komory a Vaší pojišťovny. V případě, pokud incident způsobil škodu třetí osobě nebo osobám, může být Vaše Společnost za takovou škodu trestně i finančně odpovědná. Jste na takový incident a hrozbu následků dostatečně připraveni ? Obhájíte dostatečně splnění svých povinností před vyšetřovateli ? Budou Vám klást následující otázky a Vy máte prostřednictvím našeho dotazníku možnost si odpovědi předem připravit.**

**Jméno Společnosti :**

**Adresa :**

**IČO :**

**Uveďte všechny webové stránky a domény, které Společnost a její sesterské či dceřinné společnosti používají :**

**Uveďte počet zaměstnanců :**

**Uveďte počet IT zařízení :** **serverů** **stolních PC** **notebooků** **mobil.telefonů**

## 1. POSTUPY OCHRANY ÚDAJŮ

**1.1 Podléhá Vaše Společnost pravidlům Evropské unie pro nakládání a zpracování osobních údajů ?**

○ Ano ○ Ne

**Pokud „Ne“, uveďte prosím zemi, jejímž pravidlům podléháte**

**1.2 Provedla Společnost revizi postupů ve vztahu ke zpracování údajů a zjistila oblasti, které mohou působit problémy s dodržováním postupů dle GDPR a přijala nebo přijímá přiměřená technická a organizační opatření k tomu, aby byla v souladu s GDPR řádně dokumentovaným způsobem ?**

○ Ano ○ Ne ○ Zajišťuje TECHTERRA

**1.3 Je společnost povinna jmenovat osobu odpovědnou za ochranu osobních údajů ?**

○ Ano ○ Ne ○ Zajišťuje TECHTERRA

**Pokud „Ano“, uveďte prosím identifikační údaje a sídlo této odpovědné osoby. Pokud „Ne“, kdo odpovídá za bezpečnost osobních údajů a jiných údajů a za dodržování legislativy ?**

**1.4 Přijala Společnost interní postup pro zajištění souladu s příslušnou legislativou ve vztahu k ochraně osobních údajů ?**

○ Ano ○ Ne ○ Zajišťuje TECHTERRA

**1.4.1 Práva subjektu údajů (např. přístup, oprava, vymazání nebo přenositelnost osobních údajů)**

○ Ano ○ Ne ○ Zajišťuje TECHTERRA

1.4.2 Podávání oznámení příslušnému úřadu pro ochranu osobních údajů ohledně incidentů ve spojitosti s bezpečností osobních údajů :

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

1.4.3 Podávání oznámení subjektu osobních údajů ohledně incidentů ve spojitosti s bezpečností osobních údajů:

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

1.5 Přijala Společnost interní postup pro zajištění pravidelné (nejméně každoroční) revize a v případě potřeby i aktualizace :

Oznámení týkajících se ochrany dat ◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Souhlasů ◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud odpověď na jednu nebo více otázek uvedených výše v tomto oddíle „Postupy ochrany osobních údajů“ zní „Ne“, prosím uveďte datum, kdy bude společnost implementovat všechny požadavky ve vztahu k GDPR

1.6 Zajišťuje Společnost bezpečné nakládání s dokumenty obsahujícími citlivé údaje (např. jejich ukládání do zamykatelných skříní)

◯ Ano ◯ Ne ◯ Metodicky zajišťuje TECHTERRA

1.7 Byli všichni zaměstnanci obeznámeni s opatřeními týkajícími se ochrany osobních údajů ?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

1.8 Pokud Společnost vykonává činnosti v sektorech, kde dochází ke zpracování osobních údajů dle zvláštního právního předpisu (např. poskytování zdravotních služeb; poskytování komunikačních a telekomunikačních služeb; dodávky a distribuce elektrické energie, plynu, vody, atd.; poskytování bankovních a platebních služeb; pojišťovací služby, zprostředkování pojišťovacích služeb aj.), monitoruje Společnost dodržování zvláštních zákonných povinností týkajících se ochrany osobních údajů v souladu s příslušnou legislativou?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

## 2. KVALITA A MNOŽSTVÍ DAT

2.1 Jaký typ citlivých údajů Vaše Společnost uchovává a zpracovává ?

☐ Osobní identifikovatelné informace ☐ Informace o platebních kartách

☐ Osobní informace o zdravotním stavu ☐ Uživatelská jména a hesla

Pokud je výše zvolena možnost „Informace o platebních kartách“, splňuje společnost bezpečnostní standard PCI DSS (Payment Card Industry Data Security Standards)? ◯ Ano ◯ Ne

Pokud jsou zvoleny OIÚ, IPK a OIZS je přístup k takovým citlivým údajům omezený? ◯ Ano ◯ Ne

2.2 Kontrolujete/zpracováváte osobní údaje občanů USA (kdekoli) nebo zpracováváte/kontrolujete osobní údaje v datových centrech umístěných v USA ?

◯ Ano ◯ Ne Pokud „ANO“ má příjemce osobních údajů platnou registraci v systému Privacy Shield Framework ? ◯ Ano ◯ Ne

2.3 Uveďte odhadovaný objem citlivých údajů (počet záznamů), který Vaše společnost uchovává/zpracovává :

◯ Méně než 1 000 ◯ 1 000 až 10 000 ◯ 10 000 až 100 000 ◯ více než 100 000

## 3. DIGITÁLNÍ OBSAH V MULTIMÉDIÍCH

3.1 Jaké z následujících elektronických/online činností Společnost provozuje?

☐ Publikování vlastního elektronického obsahu

☐ Obsah na základě licence od třetí strany

☐ Streaming video nebo hudební obsah na základě písemných licenčních smluv/souhlasů

☐ Poskytování poradenství (zdravotní, právní atd.)

☐ Sběr citlivých údajů (PII/PCI/PHI, IP, jiné)

☐ Nelicencovaný obsah třetich stran (např. chatovací místnosti, blogy, nástěnky, zákaznické recence atd.)

☐ Prezentace produktů/služeb druhých stran (reklama, nákup nebo prodej)

☐ Soubory ke stažení

3.2 Poskytuje web Společnosti ochranu soukromí (ohledně sběru dat, používání cookies atd.), uvádí zákonné oznámení o užívání práv třetích stran a odkazy na externí stránky, včetně prohlášení o zřeknutí se odpovědnosti (tzv. disclaimer) a je takový obsah schválen kvalifikovaným právním poradcem?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

## 4. SLUŽBY TŘETÍCH STRAN

4.1 Využívá Společnost subdodavatelů na jakoukoli část sítě, počítačového systému nebo funkcí na zabezpečení údajů?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

4.2 Požaduje Společnost, aby organizace poskytující sběr dat nebo zpracovávání údajů (subdodavatelé) udržovali také své pojištění odpovědnosti ve vztahu k ochraně údajů?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

4.3 Máte podepsanou písemnou smlouvu s příslušnými poskytovateli služeb, včetně dohody o mlčenlivosti, a provádí společnost pravidelně audit funkcí subdodavatele, aby zajistila, že se řídí bezpečnostními předpisy společnosti? Zaškrtněte N/A (nehodí se), jen pokud nemáte subdodavatele na žádnou část své sítě, počítačového systému nebo funkcí zabezpečení informací.

◯ Ano ◯ Ne ◯ N/A ◯ Zajišťuje TECHTERRA

4.4 Zaškrtněte vše, co se hodí, a uveďte organizaci poskytující služby:

☐ Řízení celého IT systému ◯ Zajišťuje TECHTERRA

☐ Offsite zálohování a uchovávání ◯ Zajišťuje TECHTERRA

☐ Zpracovávání dat ◯ Zajišťuje TECHTERRA

☐ Poskytovatel aplikační služby ◯ Zajišťuje TECHTERRA

☐ Jiné cloudové výpočetní služby: ◯ Zajišťuje TECHTERRA

## 5. IT BEZPEČNOST

5.1.1 Má Společnost odpovědnou osobu nebo tým v oblasti IT bezpečnosti, který pravidelně podává hlášení vyššímu managementu?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.2 Má Společnost zavedené formální procesy risk managmentu v oblasti IT / OT bezpečnosti?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.3 Vykonává společnost analýzu rizik před zavedením nových systémů a software?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.4 Analyzuje Společnost projekty a postupy z hlediska bezpečnosti dat jak ve fázi plánování, tak i při každé změně prvků IT prostředí?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.5 Má Společnost zavedené postupy pro správu a zjišťování zranitelností?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.6 Záplaty kritických zranitelností (CVSS Base Score ≥ 9.0) jsou nasazeny nejdéle do 7 dní od jejich vydání, popř. jsou tyto zranitelnosti ošetřeny jinak, dle doporučení vývojáře?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.7 Zaznamenává Společnost změny v IT systémech?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.8 Má Společnost zdroje (procesy, lidské zdroje, IT prvky, výrobní prvky, data, nemovitost apod.) rozdělené do kategorií důležitosti a identifikovala kritické body?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.9 Má Společnost v písemné formě plán postupů chování v případě bezpečnostního incidentu (v oblasti IT rizik) nebo narušení bezpečnosti údajů (Incident Response Plan)?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.10 Jsou přístupy zaměstnanců do firemních systémů po ukončení pracovního poměru okamžitě deaktivovány?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.11 Přidělujete při zřizování servisních účtů nejužší nezbytná práva?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.12 Práva lokálních admin účtů jsou standardně vypnuta?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.13 Přístup k lokálním admin účtům je chráněn bezpečným, unikátním heslem, který uživatel nezná.

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.14 Všichni administrátoři mají pro své administrátorské úkoly zvláštní, privilegované uživatelské účty (vedle svých běžných, uživatelských účtů pro jinou práci - běžný přístup, email, browsing apod.)?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.15 Tier 0 administrátoři (např. Domain Admin, Enterprise Admin) se mohou přihlašovat pouze do DC (Domain Controller) a Domain Admin přístup není používán pro přihlašování ke klientům běžných uživatelů či serverů.

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.16 Provádí Společnost bezpečnostní dohled / monitoring nad zaměstnanci (resp. jejich IT vybavením) pracujícími na dálku (např. home office)?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.17 Školíte pravidelně své zaměstnance ohledně povědomí v oblasti IT bezpečnosti a připravujete zaměstnance, aby byli odolnější a ostražitější vůči phishingu?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.18 Máte normu pro vytváření hesel a je prosazována, např. co se týče složitosti (silná hesla) a změn (pravidelné změny)?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Jaká je vyžadována frekvence změny hesel ? ◯ 90 dnů a méně ◯ Více než 90 dnů

Je minimální délka hesel alespoň 8 znaků ? ◯ Ano ◯ Ne

5.1.19 Maximální doba výpadku činností, než dojde k závažnému dopadu na činnost.

☐ 12 hodin ☐ 18 hodin ☐ 24 hodin ☐ 36 hodin

5.1.20 Provádí Společnost posilování bezpečnosti všech serverů a pracovních stanic? Dochází k pravidelnému odstraňování zbytečného softwaru, loginů, služeb?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.21 Jsou logy událostí z identity services (např. AD, serverů a klientů) a systémů zabezpečení IT uchovávány nejméně 60 dní a je na kritická upozornění ze systémů zabezpečení IT (firewallů atd.) reagováno nejpozději následující pracovní den?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.1.22 Má Společnost zavedenu koncepci dispečerského řízení a sběru dat (tzv. SCADA – Supervisory control and data acquisition) pro klíčovou infrastrukturu a výrobní/provozní technologické procesy?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ano“, přijala Společnost interní postupy pro zajištění pravidelných revizí a upgrade tohoto systému před napadením ? ◯ Ano ◯ Ne

5.1.23 Provedla společnost bezpečnostní audit zaměřený na IT a cyber rizika?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud je odpověď na otázku výše „Ano”, pak:

Kdy byl tento audit realizován?

Jaké byly výsledky auditu?

Byla doporučení z auditu realizována? ◯ Ano ◯ Ne

5.2.1 Používáte antivirus, anti-spyware nebo ekvivalentní ochranu proti malwaru? (profesionální nástroje, ne volně dostupné bezplatné a obdobné verze)?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ano“, jsou vaše antivirové programy stahovány a aktualizovány automaticky? ◯ Ano ◯ Ne

Je ochrana před malwarem nastavena tak, aby blokovala podezřelé logy, procesy a soubory místo toho aby jen upozorňovala na hrozby? ◯ Ano ◯ Ne

5.2.2 Jsou všechny přístupové body pro internet do vaší sítě zabezpečeny firewallem?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Jak často je konfigurace/nastavení firewallů kontrolována?

5.2.3 Monitoruje Společnost své sítě a počítačové systémy na narušení datové bezpečnosti?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.2.4 Používá Společnost řešení pro detekci a prevenci průniků do IT struktur?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ano“, tak jaká?

5.2.5 Používá Společnost řešení pro reakci na koncových bodech?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ano“, tak jaká?

Je toto řešení použito pro všechny klienty a servery? ◯ Ano ◯ Ne

Je toto řešení automaticky aktualizováno? ◯ Ano ◯ Ne

Je zavedena okamžitá reakce na kritické alerty? ◯ Ano ◯ Ne

5.2.6 Má Společnost sítě segmentovány a rozděleny dle kritičnosti?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.2.7 Používá Společnost system Zero Trust?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.2.8 Používá Společnost systém(y) a/nebo SW pro zabránění neoprávněného přístupu, detekci nebo prevenci ztráty dat?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ano“, tak jaké?

5.2.9 Má Společnost požadavky na šifrování dat při jejich předávání a uchovávání pro zajištění integrity citlivých údajů, včetně údajů na přenosných médiích (např. laptopy, DVD zálohy, kazety, pevné disky, USB zařízení, tablety, chytré telefony atd.)?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Jsou data na přenosných počítačích šifrována? ◯ Ano ◯ Ne

Jsou data při přenosu přes síť šifrována? ◯ Ano ◯ Ne

5.2.10 Je povoleno používání soukromých přenosných médií?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.2.11 Vyžaduje Společnost, aby vzdálení uživatelé byli ověřeni, než se mohou připojit k interním sítím a počítačovým systémům?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.2.12 Zajišťujete pravidelně, aby datové zálohy bylo možné obnovit co nejrychleji a s minimálním dopadem?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ano“, jakou dobu potřebujete na plné obnovení klíčových systémů a dat?

☐ Méně než 8 hodin ☐ 8–24 hodin ☐ 24–48 hodin ☐ Více než 48 hodin

5.2.13 Provádíte pravidelné automatické zálohování u klíčových systémů a dat?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ano“, jak často? ◯ Nejméně jednou denně ◯ Nejméně jednou týdně

Jsou zálohy šifrovány? ◯ Ano ◯ Ne ◯ Částečně

Jsou zálohy ukládány offline? ◯ Ano ◯ Ne ◯ Částečně

Jsou zálohy ukládány fyzicky mimo prostory společnosti? ◯ Ano ◯ Ne ◯ Částečně

5.2.14 Používá Společnost multifaktorové ověřování přístupu?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ano“, tak jaká a ve kterých systémech?

5.2.15 Je multifaktorové ověření nasazeno na všech interních přístupech systémových administrátorů (obcházení MFA za použití admin access nástrojů jako PsExec nebo Remote Powershell není možné)?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

5.2.16 Je konfigurace Active Directory kontrolována kvůli bezpečnostním nedostatkům alespoň jednou ročně za použití k tomu určených nástrojů (Bloodhound, Pingcastle, Tenbale Identity Exposure apod.) aby došlo k odhalení miskonfigurací a jejich opravě dle kritičnosti?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

## 6. DALŠÍ ZABEZPEČENÍ

6.1 Má Společnost zavedeny prvky fyzické bezpečnosti?

◯ Ano ◯ Ne Pokud „Ano”, tak jaké?

☐ Fyzická ochrana/ostraha ☐ Systém kontroly vstupu

☐ Systém detekce narušení (prostorová čidla) ☐ Kamerový systém (CCTV) se záznamem

6.2 Používá Společnost systémy / SW s ukončenou životností a pro který už není poskytována podpora?

◯ Ano ◯ Ne Pokud „Ano”, tak jaké?

O který SW/systémy se jedná ?

Ve kterých systémech Společnosti je uvedené nainstalováno ?

Jsou tyto systémy připojeny k veřejné internetové síti ? ◯ Ano ◯ Ne

Mají tyto systémy zvláštní zabezpečení ? ◯ Ano ◯ Ne

Pokud „Ano“ tak jaké ?

6.3 Umožňuje Společnost vzdálený přístup k interním systémům a zdrojům?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ano", tak:

Pomocí kterých protokolů (řešení)?

Jak je tento přístup zabezpečený?

Musí zařízení připojující se k vnitřní síti zvenčí splňovat Bezpečnostní požadavky definované Společností? ◯ Ano ◯ Ne

Monitoruje Společnost VPN zabezpečení a vede soupis (log) vzdálených přístupů zaměstnanců? ◯ Ano ◯ Ne

6.4 Má Společnost systémy průmyslové automatizace (OT)?

◯ Ano ◯ Ne

6.5 Je implementována datová dioda mezi OT a IT (Purdue model, úroveň 3 a 4)?

◯ Ano ◯ Ne

6.6 Je monitorována propustnost z IT do OT?

◯ Ano ◯ Ne

6.7 Mají OT systémy (Purdue Model, úroveň 0–3) přístup do vnější sítě?

◯ Ano ◯ Ne

Pokud „Ano", jak je tento přístup zabezpečený ?

6.8 Umožňuje Společnost vzdálený přístup třetích stran k OT systénům?

◯ Ano ◯ Ne

Pokud „Ano", tak - je vyžadován explicitní souhlas Společnosti/odborného oddělení ◯ Ano ◯ Ne

- je tento přístup plně monitorován ? ◯ Ano ◯ Ne

6.9 Jsou Distributed Control Systems/Document Management Systems pravidelně testovány z pohledu zabezpečení?

◯ Ano ◯ Ne

6.10 Používá se při analýze rizik pro OT metoda PHA/HAZOP, nebo jiná metodika odhadu a analýzy rizik?

◯ Ano ◯ Ne

6.11 Má Společnost implementovány doporučení z normy IEC 62443?

◯ Ano ◯ Ne

Pokud „Ano", jaká je SL hodnota pro dotčené systémy?

6.12 Má Společnost implementovány standardy Industry 4.0 nebo Smart Grids?

◯ Ano ◯ Ne

6.13 Využívá Společnost IoT nebo OT s prvky IoT?

◯ Ano ◯ Ne

Pokud „Ano“, tak - jsou tato zařízení/systémy připojeny ke cloudu ? ◯ Ano ◯ Ne

- jedná se o veřejný nebo soukromý cloud (nebo dediková oblast ve veřejném cloudu) ◯ Ano ◯ Ne

## 7. EOL/EOS A CVE

7.1 Máte zavedené kontrolní procesy zaměřené na SW a Aplikace po ukončení životnosti, nebo s ukončenou podporou (End of Life/End of Support) s cílem identifikovat uvedený SW/Aplikace a minimalizovat rizika vyplývající z uvedeného stavu?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

7.2 Máte zavedené procesy zaměřené na kontrolu nových zranitelností (CVE - Common Vulnerabilities and Exposures) a co nejrychlejší řešení možných ohrožení?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

## 8. AKUTNÍ ZRANITELSNOSTI

8.1 Provozuje vaše Společnost nebo využívá nějaké systémy, které jsou zranitelné vůči Log4Shell (CVE-2021-44228)?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ne“, prověřili jste toto s vaším externím dodavatelem IT služeb? ◯ Ano ◯ Ne

Pokud „Ano“, byly tyto systémy opraveny nebo byla nasazena dočasná zmírnění či kompenzace? ◯ Ano ◯ Ne

8.2 Jaké % ze zranitelných aplikací/systémů bylo opraveno? _____ %

8.3 Máte plán pro zmírnění rizik? Existuje pro tento plán časová osa?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

8.4 Provedli jste kontrolu zranitelných IT systémů vůči Indikátorům kompromisu (Indicators of Compromise - IoC)?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Byly podniknuty nezbytné kroky v případě potřeby? ◯ Ano ◯ Ne

8.5 Jaká detekční opatření jste zavedli?

8.6 Implementovali jste nějaké skenovací nástroje pro detekci log4j/log4shell?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

## 9. BUSINESS CONTINUITY PLAN (BCP)

9.1 Má vaše Společnost zavedený BCP / Plán na zachování provozu (zaměřený na IT a cyber rizika)?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud ano, kým byl tento plán vypracován a připraven?

9.2 Je BCP v souladu a dle parametrů stanovených v ISO 22301?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

9.3 Byl BCP hloubkově otestován?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ano“, tak kdy a jakým způsobem?

Kdo (pozice) prováděl kontrolu a testování BCP?

9.4 Pokrývá BCP i situace úplného výpadku/selhání interních IT sítí a zařízení?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

9.5 Pokrývá BCP i situace vyřazení/znefunkčnění kritického HW (bricking) a jeho fyzickou náhradu?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

9.6 Zajišťujete pravidelně, aby datové zálohy bylo možné obnovit co nejrychleji a s minimálním dopadem?

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

Pokud „Ano“, jakou dobu potřebujete na plné obnovení klíčových systémů a dat?

☐ Méně než 8 hodin ☐ 8–24 hodin ☐ 24–48 hodin ☐ Více než 48 hodin

## 10. BEZPEČNOSTNÍ UDÁLOSTI A HISTORIE ZTRÁT

10.1 Došlo ve Společnosti v posledních třech letech k narušení IT bezpečnosti, poškození sítě, systému nebo ztrátě dat?

◯ Ano ◯ Ne

Pokud „Ano“, jaká byla finanční ztráta Vaší společnosti v důsledku této události ?

☐ Méně než 1 mil. Kč ☐ 1 mil. Kč až 5 mil. Kč ☐ Více než 5 mil. Kč

**10.2 Došlo v posledních třech letech k oznámení ze strany zákazníka, že jeho údaje byly zneužity?**

◯ Ano ◯ Ne **Pokud „Ano“, jaká byla finanční ztráta Vaší společnosti v důsledku této události ?**

☐ Méně než 1 mil. Kč ☐ 1 mil. Kč až 5 mil. Kč ☐ Více než 5 mil. Kč

**10.3 Byla Společnost vyšetřována nebo podrobena auditu ve vztahu k ochraně údajů ze strany úřadu na ochranu údajů nebo jiného regulátora?**

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

## 11. POJIŠTĚNÍ

**11.1 Je Vaše Společnost pojištěna na škody, vzniklé narušením IT bezpečnosti, poškozením sítě, systému nebo ztrátou dat?**

◯ Ano ◯ Ne ◯ Zajišťuje TECHTERRA

**Pokud „Ano“, na jakou maximální výši škody je Vaše pojistná smlouva uzavřena ?**

☐ Méně než 1 mil. Kč ☐ 1 mil. Kč až 5 mil. Kč ☐ 5 mil. Kč až 10 mil. Kč ☐ Více než 10 mil. Kč

**DIGITERRA**

Je moderní vzdělávací institut zaměřený na přípravu jednotlivců i organizací na digitální výzvy současnosti. Specializuje se na **rekvalifikační a profesní kurzy v oblasti kybernetické bezpečnosti a umělé inteligence**, které odpovídají aktuálním požadavkům trhu služeb a práce.

**TECHTERRA**

Společnost vznikla jako servisní organizace DIGITERRA INSTITUTE s cílem **propojit výuku s praxí**. Umožňujeme svým studentům a absolventům rozvíjet a uplatnit své dovednosti v reálném prostředí, pod vedením zkušených odborníků a ve spolupráci s partnery z praxe.

**TERRACLINIC**

Portál TERRACLINIC funguje jako digitální tržiště, které propojuje zadavatele drobných zakázek z řad klientů s našimi studenty a absolventy. Ti zde získávají možnost aplikovat své znalosti v praxi, rozvíjet své schopnosti na skutečných úkolech a zároveň si přivydělat. Spolupráce probíhá pod odborným dohledem institutu.