MARSH

DOTAZNÍK

POJIŠTĚNÍ **KYBERNETICKÝCH RIZIK**

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES

MARSH

Tento dokument slouží společnosti MARSH, s.r.o. pro získání potřebných informací k poptání pojištění rizik spojených s informačními systémy žadatele. Podpis tohoto dotazníku nezavazuje pojistitele ani žadatele k uzavření pojistné smlouvy. V případě, že se standardy bezpečnosti informačních systémů liší pro jednotlivé dceřiné společnosti žadatele, vyplňte prosím dotazník pro tyto společnosti zvlášť.

1. Informace o zájemci o pojištění

Obchodní firma:

Město:

PSČ:

Webové stránky:

Počet zaměstnanců:

Roční obrat:

Roční hrubá marže:

Procento tržeb plynoucí z aktivit v:

ČR:

EU:

USA/Kanada:

Zbytek světa:

2. Profil zájemce/ů o pojištění

2.1 Předmět podnikání

Prosím popište hlavní předmět podnikání zájemce. Pokud vykonává činnosti zahrnující e-commerce, uveďte procento tržeb plynoucí z těchto aktivit.

2.2 Společnosti, které mají být pojištěny

Uveďte společnosti a dceřiné společnosti. Pokud působí dceřiné společnosti mimo ČR, uveďte podrobnosti.

2.3 Závislost podnikání na informačních systémech

Prosím zhodnoťte, při jakém výpadku by došlo k významnému ovlivnění vašeho podnikání.

	Minimální délka výpadku, který negativně ovlivní podnikání				
Aplikace/činnost	Okamžitě	>12 h	>24 h	>48 h	>5 den

3. Informační systémy

	<100	101-1000	>1000
Počet uživatelů informačních systémů			
Počet notebooků			
Počet serverů			

Nabízíte své služby online pomocí webových stránek či e-commerce? ☐Ano ☐No

Pokud ano, jaké procento na celkových výnosech generují online služby?(odhad) (% nebo mKč)

4. Bezpečnost informací (IS)

4.1 Bezpečnostní politika a řízení rizik (risk management)

1	Politika bezpečnosti informací je formálně schválena managementem společnosti a/nebo pravidla bezpečnosti jsou jasně definována a komunikována všem zaměstnancům a odsouhlasena jejich zástupci	☐Ano	☐Ne
2	Školení o bezpečnosti informací je vyžadováno pro všechny zaměstnance alespoň jednou ročně	☐Ano	☐Ne
3	Identifikujete kritická rizika informačních systémů a podnikáte vhodné kroky k jejich zmírnění	☐Ano	☐Ne
4	Provádíte pravidelnou kontrolu informačních systémů a implementujete vyplývající doporučení	☐Ano	☐Ne
5	Informační zdroje jsou inventarizovány a klasifikovány podle jejich kritičnosti a citlivosti	☐Ano	☐Ne
6	Požadavky na bezpečnost, které se týkají informačních zdrojů, jsou definovány podle stupně utajení/citlivosti	☐Ano	☐Ne

4.2 Ochrana informačních systémů

1	Přístup do kritických informačních systémů vyžaduje dvojí ověření	☐Ano	☐Ne
2	Uživatelé musí pravidelně aktualizovat svá hesla	☐Ano	☐Ne
3	Autorizace pro přístup závisí na roli uživatele a je zaveden postup pro její správu	☐Ano	☐Ne
4	Existují referenční nastavení/příručky pro ukázkové nastavení pro pracovní stanice, notebooky, servery a mobilní zařízení (přístroje)	☐Ano	☐Ne
5	Je zavedena centralizovaná správa a monitoring konfigurace počítačových systémů	☐Ano	☐Ne
6	Notebooky jsou chráněny osobním firewallem	☐Ano	☐Ne
7	Antivirový program je nainstalován na všech systémech a jeho aktualizace jsou monitorovány	☐Ano	☐Ne
8	Pravidelně jsou nasazovány bezpečnostní softwarové aktualizace	☐Ano	☐Ne
9	Existuje plán obnovy činnosti po havárii a je pravidelně aktualizován	☐Ano	☐Ne
10	Zálohování dat se provádí denně, zálohy jsou pravidelně testovány a jejich kopie pravidelně umisťovány na vzdáleném místě	☐Ano	☐Ne

4.3 Bezpečnost sítě a provozu

1	Filtrování síťového provozu mezi interní sítí a internetem je monitorováno a pravidelně aktualizováno	☐Ano	☐Ne
2	Je zaveden systém prevence a detekce narušení, který je pravidelně aktualizován a monitorován	☐Ano	☐Ne
3	Interní uživatelé přistupují k internetovým stránkám přes síťové zařízení (proxy) vybavené antivirem a filtrem internetového obsahu	☐Ano	☐Ne
4	Síť je segmentována za účelem oddělení kritických oblastí od nekritických	☐Ano	☐Ne
5	Penetrační testy jsou prováděny pravidelně a v případě potřeby je implementován plán nápravy	☐Ano	☐Ne
6	Hodnocení chyb zabezpečení je prováděno pravidelně a v případě potřeby je implementován plán nápravy	☐Ano	☐Ne
7	Jsou implementovány postupy pro správu incidentů a řízení změn	☐Ano	☐Ne
8	Bezpečnostní události jako například detekce viru, pokusy o přístup, atd. jsou zaznamenávány a pravidelně monitorovány	☐Ano	☐Ne

4.4 Fyzické zabezpečení servrovny

1	Kritické systémy jsou umístěny v alespoň jedné vyhrazené místnosti s omezeným přístupem a provozní alarmy jsou svedeny do monitorovacího místa	☐Ano	☐Ne
2	Datové centrum hostující kritické systémy má odolnou infrastrukturu včetně redundatní dodávky energie, klimatizace a síťového připojení	☐Ano	☐Ne
3	Kritické systémy jsou v klastru typu Aktiv/Pasiv nebo Aktiv/Aktiv architektury	☐Ano	☐Ne
4	Kritické systémy jsou duplikovány ve dvou oddělených lokalitách	☐Ano	☐Ne
5	Detekce požáru a automatický systém hašení v kritických oblastech	☐Ano	☐Ne
6	Dodávka proudu je chráněna UPS a bateriemi a je v pravidelné údržbě	☐Ano	☐Ne
7	Napájení je zálohováno elektrickým generátorem, jež je pravidelně udržován a testován	☐Ano	☐Ne

4.5 Outsourcing

[Prosím vyplňte, pokud využíváte outsourcing]

1	Smlouva o outsourcingu obsahuje požadavky na zabezpečení, jež by měly být dodržovány poskytovatelem služby	☐Ano	☐Ne
2	S poskytovatelem služby je dohodnuta správa úrovní služeb (SLA – Service Level Agreement), aby bylo umožněno řízení incidentů a změn. V případě nedodržení jsou aplikovány sankce vyjmenované v SLA	☐Ano	☐Ne
3	Monitorovací a řídící výbor(y) jsou organizovány ve spolupráci s poskytovatelem služeb pro řízení a zlepšování služeb	☐Ano	☐Ne
4	Nevzdali jste se svých práv na náhradu škody vůči poskytovali služeb ve smlouvě o outsourcingu	☐Ano	☐Ne

Jaké jsou funkce outsourcovaného informačního systému?			**Poskytovatel služby (outsourcer)**
Správa klientských stanic	☐Ano	☐Ne	
Správa serveru	☐Ano	☐Ne	
Správa sítě	☐Ano	☐Ne	
Správa bezpečnosti sítě	☐Ano	☐Ne	
Správa aplikací	☐Ano	☐Ne	
Využití cloudu	☐Ano	☐Ne	
Pokud ano, specifikujte charakter cloudových služeb			
SAS (Software as a Service)	☐Ano	☐Ne	
PAS (Platform as a Service)	☐Ano	☐Ne	
IAS (Infrastructure as a Service)	☐Ano	☐Ne	

Jiné:

5 Smlouva o outsourcingu zahrnuje ustanovení o povinnosti poskytovatele služby sjednat pojištění profesní odpovědnosti ☐Ano ☐Ne

5. Osobní údaje držené nebo uložené v organizaci

5.1 Typ a počet záznamů

Pro účely tohoto pojištění uveďte počet záznamů s osobními informacemi vedené společností

Celkem:

Dle oblastí:

ČR:

EU:

USA/Kanada:

Zbytek světa:

Kategorie shromažďovaných a zpracovávaných osobních údajů:

			Počet záznamů
Obchodní a marketingové informace	☐Ano	☐Ne	
Informace o platebních kartách nebo finančních transakcích	☐Ano	☐Ne	
Zdravotní údaje	☐Ano	☐Ne	

Jiné:

Zpracováváte data: ☐ Pro vlastní účely? ☐ Jménem třetích stran?

5.2 Standardy ochrany osobních údajů

1	Zásady ochrany osobních údajů jsou formalizovány a odsouhlaseny vedením společnosti a předpisy pro jejich zabezpečení jsou definovány a komunikovány dotčeným zaměstnancům	☐Ano	☐Ne
2	Školení jsou poskytována nejméně jednou ročně osobám oprávněným k přístupu nebo zpracovávání osobních údajů	☐Ano	☐Ne
3	Společnost určila pověřenou osobu pro ochranu osobních údajů	☐Ano	☐Ne
4	Dohoda o zachování důvěrnosti informací nebo klauzule o mlčenlivosti v pracovní smlouvě je podepsána příslušnými zaměstnanci	☐Ano	☐Ne
5	Právní aspekty politiky ochrany osobních údajů jsou ověřeny právníkem/právním oddělením	☐Ano	☐Ne
6	Monitoring je prováděn s cílem zajistit soulad s právními předpisy o ochraně osobních údajů	☐Ano	☐Ne
7	Postupy nakládání s osobními údaji byly v posledních dvou letech auditovány externím auditorem	☐Ano	☐Ne
8	Reakční plán při porušení ochrany údajů je zaveden a role jsou jasně komunikovány členům týmu	☐Ano	☐Ne

5.3 Shromažďování osobních údajů

1	Oznámili jste zpracovávání osobních dat Úřadu pro ochranu osobních údajů a ten vám udělil příslušné oprávnění	☐Ano	☐Ne
2	Zásady ochrany osobních údajů jsou zveřejněny na vašich webových stránkách, které byly revidovány právníkem/právním oddělením	☐Ano	☐Ne
3	Je zapotřebí souhlas osob, jejichž osobní údaje mají být shromážděny a dotčené osoby mají k těmto údajům přístup, aby je mohly v případě potřeby opravit nebo vymazat	☐Ano	☐Ne
4	Příjemcům jsou poskytovány jednoznačné prostředky k odhlášení se z cílených marketingových akcí	☐Ano	☐Ne
5	Předáváte osobní údaje třetím stranám. Pokud ano, odpovězte prosím následující:	☐Ano	☐Ne
	a) Třetí strana má smluvní odpovědnost zpracovávat osobní data jen vaším jménem a dle vašich pokynů	☐Ano	☐Ne
	b) Třetí strana má smluvní odpovědnost vytvořit dostatečná bezpečnostní opatření k ochraně osobních údajů	☐Ano	☐Ne

5.4 Kontrola ochrany osobních údajů

1	Přístup k osobním údajům je omezen pouze na ty uživatele, kteří jej potřebují k plnění svých pracovních úkolů a přístupová oprávnění jsou pravidelně revidována	☐Ano	☐Ne
2	Osobní data jsou šifrována při uložení do informačních systémů a zálohy těchto dat jsou též šifrovány	☐Ano	☐Ne
3	Osobní data jsou zašifrována při přenosu po síti	☐Ano	☐Ne
4	Mobilní zařízení a pevné disky notebooků jsou šifrovány	☐Ano	☐Ne
5	Politika bezpečnosti informací zakazuje kopírování nešifrovaných osobních údajů na výměnná paměťová zařízení nebo přenos těchto dat pomocí e-mailu	☐Ano	☐Ne

Pokud osobní záznamy obsahují informace o platebních kartách (dále jen PCI), zodpovězte prosím následující:

Úroveň PCI DSS: Úroveň 1 Úroveň 2 Úroveň 3 Úroveň 4 Zpracovávatel plateb (Vy nebo třetí strany) je v souladu s PCI DSS ☐Ano ☐Ne

Pokud ne:

PCI jsou uloženy zašifrované nebo je uložena pouze část čísel platebních karet ☐Ano ☐Ne

Doba držení PCI nepřekračuje dobu trvání platby a zákonných / regulačních požadavků ☐Ano ☐Ne

Zpracování údajů platebních karet je externalizováno ☐Ano ☐Ne

Pokud ne:

Vyžadujete od zpracovatele plateb, aby vás v případě porušení bezpečnosti odškodnil ☐Ano ☐Ne

Prosím uveďte identifikační údaje zpracovatele plateb, dobu držení PCI a jakékoli další bezpečnostní opatření:

Click here to enter text.

5.5 Incidenty/ Incidents

Prosím popište jakékoli události týkající se bezpečnosti dat a osobních údajů, které se udály během posledních 36 měsíců. Incidenty zahrnují jakýkoli nepovolený přístup k jakémukoli počítači, výpočetní technice, databázi, narušení či útoky, odmítnutí použití jakéhokoliv počítače nebo systému, úmyslné narušení, poškození nebo zničení dat, programů nebo aplikace, jakékoliv vydírání nebo jiné události podobné výše uvedenému, včetně těch, které vedly k nároku, správnímu nebo regulačnímu řízení.

Datum **Popis incidentu**

Komenář

Žádná osoba nebo entita navržená do pojistného krytí si není vědoma jakékoli skutečnosti, okolnosti nebo situace, která by mohla vést ke vznesení nároku, jež by byl řešen z titulu navrhovaného pojištění.

☐Žádný subjekt

☐Nebo kromě:

Kontaktní osoby pro doplňující informace

Jméno:

Titul:

Telefonní číslo:

E-Mail:

Zpracováno:

Zájemce o pojištění po pečlivém prostudování tohoto dotazníku prohlašuje a potvrzuje, že výše uvedené odpovědi na dotazy a poskytnuté informace jsou pravdivé a úplné a žádné údaje nejsou nesprávné a nebyly zamlčeny nebo vynechány. Zájemce o pojištění se tímto zavazuje k povinnosti informovat pojistitele o jakýchkoliv důležitých změnách v informacích poskytnutých v tomto dotazníku, které mohou nastat před nebo po uzavření pojistné smlouvy, k níž se tento dotazník vztahuje. Zájemce o pojištění tímto také bere na vědomí, že tento dotazník (společně s dalšími podklady a informacemi poskytnutými pojistiteli) bude podkladem k uzavření takové pojistné smlouvy.

Zájemce o pojištění tímto také bere na vědomí, že pojistitel spoléhá na údaje uvedené v tomto dotazníku. Zájemce o pojištění tímto dále bere na vědomí, že nejsou-li dotazy a informace v tomto dotazníku zodpovězeny či poskytnuty pravdivě a úplně, má pojistitel právo postupovat dle platných právních předpisů, včetně případného odmítnutí pojistného plnění dle příslušných ustanovení zákona č. 89/2012 Sb., občanský zákoník.

Jméno a Příjmení

Funkce:

Datum:

Podpis: