PRAVIDLA INFORMAČNÍ A KYBERNETICKÉ BEZPEČNOSTI PRO DODAVATELE (PIKYB)

Obsah:

1 ZÁKLADNÍ POJMY A ZKRATKY

SMLOUVA	Smlouva o dílo/Kupní smlouva/Rámcová smlouva o poskytování služeb jejíž přílohou je tento dokument.
SYSTÉM	Služby/dodávky specifikované v Předmětu DÍLA SMLOUVY jejích přílohách.
OBJEDNATEL	Plzeňská teplárenská a.s.
Informační bezpečnost	Ochrana informací a informačních systémů před neoprávněným přístupem, užíváním, odhalením, rušením, změnou, inspekcí, záznamem nebo zničením s cílem zabezpečit jejich důvěrnost, integritu a dostupnost.
Kybernetická bezpečnost	Ochrana systémů, sítí a dat v digitálním prostoru před útoky, poškozením nebo neoprávněným přístupem. Zahrnuje implementaci technologií, postupů a strategií na ochranu elektronických informací a infrastruktury.
Prostředky OBJEDNATELE	Hmotné i nehmotné věci ve vlastnictví nebo nájmu OBJEDNATELE, které jsou nezbytné k plnění předmětu smlouvy.
Prostředí OBJEDNATELE	Fyzický perimetr určený ohraničením fyzického prostoru v nájmu nebo majetku OBJEDNATELE anebo logický perimetr definovaný hraničními prvky informačního/komunikačního systému ve správě nebo majetku OBJEDNATELE.
Prostředky ZHOTOVITELE	Hmotné i nehmotné věci ve vlastnictví nebo nájmu ZHOTOVITELE, které jsou nezbytné k plnění předmětu smlouvy.
Prostředí ZHOTOVITELE	Fyzický perimetr určený ohraničením fyzického prostoru v nájmu nebo majetku ZHOTOVITELE anebo logický perimetr definovaný hraničními prvky informačního/komunikačního systému ve správě nebo majetku ZHOTOVITELE.
VoKB	Vyhláška 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) ve znění pozdějších přepisů.
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
Osobní údaje	Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby).
Zpracování osobních údajů	Jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

2 ÚVODNÍ USTANOVENÍ

Plzeňská teplárenská, a.s. (dále jen „PLTEP“) je správcem a provozovatelem informačního a komunikačního systému kritické informační infrastruktury dle § 3 písm. c) a d), příp. f) a g) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZoKB“).

Zařízení, jehož dodávka, servis a úpravy jsou předmětem činnosti ZHOTOVITELE, je v souladu s § 2 písm. b) a k) ZoKB součástí určeného systému kritické informační infrastruktury, resp. základní služby v oblasti výroby elektrické energie a podpůrných služeb, resp. výroby tepelné energie.

3 PRAVIDLA PRO ZHOTOVITELE

Pracovník ZHOTOVITELE prohlašuje, že byl prokazatelně seznámen s podmínkami a náležitostmi Smlouvy, na základě, které bude provádět pracovní činnost pro PLTEP. Tyto podmínky se zavazuje dodržovat a dále je povinen dodržovat níže uvedená pravidla, která se vztahují na práci v prostředí OBJEDNATELE:

- s prostředky ZHOTOVITELE;
- s prostředky OBJEDNATELE;
- mimo prostředí OBJEDNATELE.

Při veškeré činnosti musí pracovník ZHOTOVITELE dodržovat předepsané a doporučené pracovní postupy a metody, aby nedošlo k narušení kybernetické bezpečnosti a bezpečnosti informací.

3.1 Fyzická bezpečnost – pohyb v areálu OBJEDNATELE

V rámci své činnosti má pracovník ZHOTOVITELE oprávnění vstupovat pouze do prostor, které jsou nezbytné pro vykonávání jeho činnosti.

ZHOTOVITEL je povinen informovat garanta smlouvy OBJEDNATELE e-mailem nejméně 24 hodin před příjezdem do areálu OBJEDNATELE. V případě nedodržení časové lhůty pro informování garanta smlouvy OBJEDNATELE o příjezdu ZHOTOVITELE nemusí být ZHOTOVITEL vpuštěn do areálu OBJEDNATELE.

3.2 Řízení do přístupu do sítě

Přidělení oprávnění přístupu do prostředí OBJEDNATELE pracovníkovi ZHOTOVITELE se řídí principem nezbytného minima a není nárokové.

Pracovník ZHOTOVITELE má zakázáno sdílet autentizační prostředky pro přístup do prostředí OBJEDNATELE s jinými osobami. Případná výjimka musí být schválena odpovědnou osobou OBJEDNATELE a musí být na straně ZHOTOVITELE evidována. Za sdílené autentizační prostředky odpovídá žádající osoba o výjimku na straně ZHOTOVITELE.

Přístupová oprávnění budou využívána výhradně k účelům splnění předmětu SMLOUVY.
Pokud má pracovník ZHOTOVITELE v rámci plnění DÍLA právo používat privilegovaná oprávnění, musí je využívat jen v přiměřené míře a jen pro dobu nezbytně nutnou pro vykonání činností v souladu s plněním předmětu SMLOUVY. Privilegovaná oprávnění nesmí být využívána pro běžnou práci.

3.3 Politika HESEL

Pracovník ZHOTOVITELE musí dodržovat předepsanou politiku hesel:

- délka hesla min. 12 znaků (uživatel) / 17 znaků (administrátor)
- kombinace malé/velké písmeno, číslice, speciální znak (alespoň 3 z uvedených)
- heslo NESMÍ obsahovat:
    - nejčastěji používaná hesla,
    - přihlašovací jméno, e-mail, název systému a obdobně
    - opakované či sekvenční sady (třeba zzzz nebo abc456)
    - jména a/nebo data narození uživatele, jeho přátel či příbuzných;
    - kombinace obsahující aktuální rok, měsíc nebo roční období (např. Summer2018);

Hesla nesmí poznamenána v čitelné formě ať už písemně nebo elektronicky (soubory, mail).
Prozrazená hesla musí být okamžitě změněna a jakékoli incidenty s vyzrazením nebo zneužitím přihlašovacích údajů musí být neprodleně ohlášeny příslušnému pracovníkovi OBJEDNATELE.
Pracovník ZHOTOVITELE, kterému je uživatelský účet přidělen, je plně odpovědný za veškeré aktivity provedené tímto účtem v počítačové síti.
Výjimka z politiky hesel musí být schválena Architektem KB OBJEDNATELE.

3.4 Požadavky na zařízení připojovaná do sítě OBJEDNATELE

Připojovat do prostředí OBJEDNATELE (ať místně do LAN nebo vzdáleně přes VPN přístup) lze pouze výslovně schválená zařízení (viz. Příloha č.1 PIKYB – Žádost o zřízení přístupu do sítě PLTEP), která musí splňovat:

- Veškerý nainstalovaný SW je legální a splňuje licenční podmínky výrobce
- Operační systém s platnou servisní podporou výrobce (vydávání bezpečnostních update)
- Funkční a pravidelně prováděné automatické aktualizace bezpečnostních záplat veškerého SW (OS, Office, JAVA, SQL, apod…)
- Funkční a pravidelně aktualizovanou antivirovou ochranou se zapnutým rezidentním štítem
- Nastavenou automatickou antivirovou kontrolu po vložení výměnných médií (USB, CD/DVD, apod)
- Funkční personální firewall s nastavením pouze nezbytných pravidel
- Musí být připojeno do sítě OBJEDNATELE na místě, které definuje OBJEDNATEL

Pokud je zařízení pracovníka ZHOTOVITELE připojeno do vnitřní sítě OBJEDNATELE, **NESMÍ** být současně připojeno k internetu (přes WiFi, LTE, mobilní Hotspot apod…).

3.5 Instalace SW

Instalovat SW do prostředí OBJEDNATELE je možné pouze po předchozím schválení instalačních postupů ze strany OBJEDNATELE.

3.6 Výměnná paměťová média

V prostředí OBJEDNATELE je povoleno používat pouze registrovaná výměnná média (USB flash, externí HDD), která jsou evidovaná. Na paměťovém médiu mohou být uloženy pouze informace a data bezprostředně související s předmětem Díla, které ZHOTOVITEL vykonává pro OBJEDNATELE. ZHOTOVITEL odpovídá za bezpečnost výměnných paměťových médií a jejich pravidelnou kontrolu po celou dobu projektu. O využívání výměnných médií souvisejících s předmětem DÍLA musí ZHOTOVITEL vést evidenci.

Data mohou na paměťovém médiu uložena pouze po nezbytně nutnou dobu (např. přenos dat mezi různými systémy), Výměnné paměťové médium nesmí být v žádném případě používána pro dlouhodobé zálohování dat a informací.

Na výměnných paměťových médiích nesmí být ukládány informace kategorie VYSOKÉ a KRITICKÉ.

3.7 Zakázané činnosti

Pracovníkům ZHOTOVITELE je zakázáno:

- bez předchozí domluvy s odpovědným pracovníkem PLTEP provádět jakékoliv činnosti na prvcích komunikační sítě OBJEDNATELE (switche, kabeláže).
- ukládat nebo sdílet data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno OBJEDNATELE;
- stahoval, sdílet/šířit, ukládat ani instalovat datové a spustitelné soubory v rozporu s licenčními podmínkami nebo s ochranou duševního vlastnictví;
- navštěvovat internetové stránky s eticky nevhodným obsahem;
- šířit spamu a obdobný nevyžádaný obsah.
- pokoušet se o jakýkoliv neautorizovaný přístup

V prostředí OBJEDNATELE je dále zakázáno instalovat nebo používat tyto typy nástrojů, pokud nejsou součástí předmětu plnění:

- Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.
- Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.
- Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT/ICS, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.
- Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT/ICS.
- Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele;
- Obdobné rizikové nástroje, který mají za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

3.8 Hlášení kybernetických bezpečnostních incidentů

ZHOTOVITEL musí bez prodlení hlásit odpovědným pracovníkům OBJEDNATELE všechna podezření na kybernetické bezpečnostní události a incidenty a spolupracovat na jejich řešení poskytnutím nezbytné součinnosti a informací/dat.

Přičemž K**ybernetickou bezpečnostní událostí** je událost, která ***<u>může způsobit narušení</u>*** bezpečnosti informací v informačních systémech, nebo narušení bezpečnosti služeb, anebo bezpečnosti a integrity sítí elektronických komunikací (tedy KB událost, která má potenciál být KB incidentem).

A **Kybernetickým bezpečnostním incidentem** je ***<u>narušení</u>*** bezpečnosti informací v informačních systémech, nebo narušení bezpečnosti služeb, anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události, tedy v zásadě každé narušení zajištění důvěrnosti, integrity a dostupnosti informací a dat a narušení dostupnosti nebo interoperability služeb a integrity sítí (tedy KB událost, u které bylo ověřeno, že jde o reálné/skutečné narušení).

3.9 Monitoring činností

Přístup a aktivity pracovníků ZHOTOVITELE k aktivům a infrastruktuře OBJEDNATELE jsou nepřetržitě zaznamenávány, monitorovány a vyhodnocovány.Pracovník ZHOTOVITELE bere na vědomí, že v případě podezření na závadné nebo nestandardní chování může být příslušný účet zablokován a případně mohou být aktivovány postupy pro zvládání bezpečnostních incidentů.

3.10 Klasifikace a pravidla nakládání s informacemi

Pracovník musí dodržovat pravidla nakládání s informacemi dle jejich klasifikace (příloha č. 2 – Pravidla ochrany kybernetických aktiv). Pokud není uvedeno jinak, veškeré informace obdržené od OBJEDNATELE se pokládají za **INTERNÍ**. V návaznosti na klasifikaci informací se musí pracovník ZHOTOVITELE řídit příslušným způsobem mazání a likvidace dat a informací dle jejich klasifikace (Příloha č. 3 PIKYB – Způsob mazání a likvidace dat a informací).