Prohlášení o kybernetické bezpečnosti

Společnosti RTS, a.s.ve vztahu k softwarovému produktu ● **BUILD** Power S

V Brně dne: 20. 11. 2025
RTS, a.s.

ÚVOD A CÍL DOKUMENTU

Společnost RTS, a.s. si je plně vědoma požadavků směrnice NIS2 (2022/2555) a zákona č. 212/2024 Sb. o kybernetické bezpečnosti. Jako subjekt působící ve vývoji a poskytování softwarových informačních systémů nesplňujeme kritéria pro zařazení mezi důležité subjekty, ani specifická riziková kritéria NÚKIB, a proto nejsme registrovaným důležitým subjektem. Přesto máme všechny relevantní opatření kybernetické bezpečnosti plně implementovány a průběžně udržované v rámci certifikovaného systému managementu bezpečnosti informací ISO/IEC 27001:2022, což překračuje standardní požadavky pro náš typ činnosti a zajišťuje vysokou úroveň ochrany pro naše zákazníky.

Společnost RTS, a.s. vyvíjí a dodává expertní software **BUILD**power S.
Tento dokument má za cíl transparentně informovat zákazníky, partnery i veřejnost o přístupu společnosti RTS, a.s. k ochraně jejich dat a systémů z pohledu kybernetické bezpečnosti, zejména v kontextu:

- způsobu distribuce a instalace softwaru **BUILD**power S,
- podmínek a omezení vzdáleného přístupu,
- certifikovaného systému managementu bezpečnosti informací podle ISO/IEC 27001:2022.

CERTIFIKACE ISO/IEC 27001:2022

Společnost RTS, a.s. je držitelem certifikátu systému managementu bezpečnosti informací podle mezinárodní normy **ISO/IEC 27001:2022**.
Rozsah certifikace: „Poskytování softwarových informačních systémů“ (tento rozsah zahrnuje veškeré činnosti spojené s vývojem, dodávkou, aktualizacemi i případnou technickou podporou produktu BUILD Power S).
Certifikace prokazuje, že RTS:

- systematicky identifikuje a vyhodnocuje bezpečnostní rizika,
- zavádí, udržuje a průběžně zlepšuje adekvátní bezpečnostní opatření (technická, organizační, personální i fyzická),
- splňuje nejvyšší mezinárodní standardy ochrany informací a kybernetické bezpečnosti.

Certifikát je vydán akreditovaným certifikačním orgánem tayllorcox.com a je pravidelně přezkušován.

MODEL DISTRIBUCE A INSTALACE SOFTWARE

UŽIVATELSKÁ INSTALACE A AKTUALIZACE

Základním a výchozím způsobem dodání softwaru BUILD Power S (včetně nových verzí a aktualizací software a cenové soustavy RTSDATA) je **samoobslužná instalace zákazníkem**.

- Zákazník stahuje instalační balíčky z oficiální zabezpečené sekce webu RTS.
- Všechny balíčky jsou podepisovány digitálním podpisem RTS (kódové podpisy Authenticode / EV Code Signing certifikát).
- Přenos probíhá výhradně přes šifrované spojení HTTPS (TLS 1.3).

Tento model eliminuje nutnost jakéhokoli přístupu zaměstnanců RTS do systémů zákazníka při běžné instalaci či aktualizaci.

VZDÁLENÝ PŘÍSTUP

Software BUILD Power S **neobsahuje žádné nedokumentované funkce**, backdoory ani mechanismy umožňující automatický vzdálený přístup ze strany RTS.
Veškerá komunikace softwaru s centrálními servery RTS (licenční kontrola, telemetrie atd.) je:

- anonymizována,
- šifrována,
- iniciována výhradně ze strany klientského softwaru (outbound spojení).

VZDÁLENÁ PODPRA PROSTŘEDNICTVÍM TEAM VIEWER

NA ŽÁDOST ZÁKAZNÍKA

V ojedinělých případech, kdy není možné problém vyřešit jinak (telefonicky, e-mailem, sdílením obrazovky přes zabezpečený firemní nástroj apod.), nabízíme vzdálenou pomoc přes software TeamViewer.

Klíčové bezpečnostní principy:

1. Relace je vždy iniciována zákazníkem – zaměstnanec RTS nemá možnost se k počítači připojit bez aktivního souhlasu a zadání jednorázového kódu.
2. Zákazník vidí veškerou aktivitu na obrazovce v reálném čase a může relaci kdykoli ukončit jediným kliknutím.
3. Veškerý přenos dat je šifrován end-to-end šifrováním AES-256.
4. Relace nejsou nahrávány ze strany RTS (pokud není výslovně dohodnuto jinak a zákazník s nahrávkou souhlasí).
5. Zaměstnanci RTS mají přísně vymezená oprávnění – přístup je povolen pouze na dobu nezbytně nutnou a pouze osobám, které prošly školením bezpečnosti a podepsaly mlčenlivost.
6. Veškeré případy vzdáleného přístupu jsou logovány (datum, čas, ID relace, jméno zaměstnance, jméno zákazníka) a podléhají internímu auditu v rámci ISO 27001.

SHRNUTÍ BEZPEČNOSTNÍCH ZÁRUK

ASPEKT	ZAJIŠTĚNÍ
Šifrovaná komunikace	1 TLS 1.3 (web), AES-256 (TeamViewer), end-to-end kde je to možné
Certifikace	ISO/IEC 27001:2022 – plný rozsah činosti
Instalace a aktualizace	Samoobslužná, HTTPS + digitální podpis, žádný přístup RTS
Vzdálený přístup	Pouze na výslovné vyžádání, iniciovaný zákazníkem, plně pod jeho kontrolou
Backdoory / nedokumentované funkce	Neexistují – prohlášení vedení společnosti čně
Transparentnost	Tento veřejně dostupný dokument