BEZPEČNOSTNÍ POLITIKA
(AL 3 + PROTOTYPY)

Tato bezpečnostní politika definuje zásady a cíle pro zajištění bezpečnosti informací, které naše organizace zpracovává v souladu s požadavky ISO/IEC 27001:2022 resp. TISAX (Trusted Information Security Assessment Exchange) na úrovni AL 3. Cílem politiky je zajistit bezpečnost informací, snížit rizika spojená s kybernetickými hrozbami a zajistit soulad s požadavky našich zákazníků a partnerů.

Tato politika se vztahuje na všechny zaměstnance, dodavatele a další osoby, které mají přístup zejména k citlivým (důvěrným nebo tajným) informacím a prototypům společnosti. Platí pro všechna aktiva, zejména zařízení, informační systémy a fyzické prostory, kde jsou data ukládána nebo zpracovávána.

HLAVNÍ BEZPEČNOSTNÍ ZÁSADY

Řízení přístupu

- Přístup k informacím a prototypům je umožněn pouze oprávněným osobám na základě role a odpovědnosti.
- Implementace vícefaktorové autentizace pro kritické systémy.
- Pravidelné revize přístupových práv a jejich odebrání při změně role nebo odchodu zaměstnance.

Ochrana dat a prototypů

- Veškerá citlivá data a prototypy jsou chráněny před neoprávněným přístupem a manipulací.
- Použití bezpečných šifrovacích algoritmů pro citlivá data.
- Zavedení kontrolních mechanismů pro sledování a evidence přístupu k prototypům.

Fyzická bezpečnost

- Kontrolovaný přístup do kritických prostor pomocí bezpečnostních prvků (RFID, kamerový systém).
- Omezený přístup k serverům, síťovým prvkům a prototypům.
- Monitorování a evidence návštěvníků.

Ochrana proti kybernetickým hrozbám

- Použití firewallů, antivirové ochrany a systémů pro detekci hrozeb.
- Pravidelné aktualizace softwaru a bezpečnostních záplat.
- Monitoring systémů a detekce anomálií.

Školení a povědomí

- Pravidelné školení zaměstnanců o bezpečnostních rizicích a postupech.
- Ochrana proti phishingovým útokům a sociálnímu inženýrství.
- Povinnost hlásit bezpečnostní incidenty.

Řízení bezpečnostních incidentů

- Definování postupu reakce na incidenty, včetně eskalačních mechanismů.
- Dokumentace všech bezpečnostních událostí a incidentů a přijatých opatření.
- Pravidelné testování krizového plánu včetně plánů kontinuity.

Vedení organizace je odpovědné za zajištění implementace a dodržování této bezpečnostní politiky. **Každý zaměstnanec** je povinen se řídit těmito zásadami a dodržovat předepsané postupy.

Porušení této politiky může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Tato politika bude pravidelně revidována alespoň jednou ročně nebo při významných změnách v oblasti informační bezpečnosti. Aktualizace budou prováděny v souladu s novými bezpečnostními požadavky a změnami v legislativě.

V Šenově dne 04.08.2025

Vedení společnosti **BREBECK Composite s.r.o.**