

### **Ustanovení týkající se kybernetické bezpečnosti**

1. Dodavatel přijme vhodná organizační a technická opatření k zajištění důvěrnosti, authenticity, integrity a dostupnosti činností dodavatele stejně jako jeho výrobků a služeb. Tato opatření budou odpovídat dobré průmyslové praxi a budou zahrnovat vhodný systém řízení Informační bezpečnosti konsistentní se standardy jako ISO/IEC 27001 nebo IEC 62443 (v použitelném rozsahu).
2. Činnostmi dodavatele se rozumí veškerý majetek, procesy a systémy (včetně informačních systémů), data (včetně zákaznických dat), personál a lokality, používané nebo zpracovávané dodavatelem čas od času za účelem plnění smlouvy.
3. Pokud výrobky nebo služby zahrnují software, firmware, nebo čipsety:
  - a) dodavatel zavede vhodné standardy, procesy a metody prevence, identifikace, vyhodnocení a oprav jakýchkoliv slabých míst, záluďných kódů a bezpečnostních incidentů u výrobků a služeb, které budou konsistentní s dobrou průmyslovou praxí a standardy ISO/IEC 27001 nebo IEC 62443 (v použitelném rozsahu),
  - b) dodavatel bude pokračovat v podpoře a poskytování služeb oprav, aktualizací, vylepšování a udržování výrobků a služeb včetně poskytování opravek objednateli napravujících slabá místa po dobu přiměřeného životního cyklu daných výrobků a služeb,
  - c) dodavatel poskytne objednateli seznam materiálů identifikujících softwarové komponenty od třetích stran obsažené ve výrobcích. Software třetích stran bude aktualizovaný ke dni dodávky objednateli,
  - d) dodavatel zaručuje objednateli právo, ale objednatel nebude povinen toto právo využít, testovat nebo nechat otestovat výrobky pro škodlivý kód nebo bezpečnostní zranitelnosti, a to kdykoliv, a adekvátně v tomto objednateli podporovat,
  - e) dodavatel poskytne objednateli kontaktní údaje pro všechny záležitosti týkající se informační bezpečnosti (dostupné v pracovní době).
4. Dodavatel bezodkladně vyrozumí objednatele o všech relevantních incidentech v oblasti informační bezpečnosti, které se stanou nebo na něž bude podezření, a o slabých místech objevených v jakémkoliv činnosti dodavatele, výrobcích či službách, pokud a v rozsahu, v jakém by objednatel byl nebo mohl by pravděpodobně být závažným způsobem dotčen.
5. Dodavatel přijme příslušná opatření k dosažení toho, že jeho subdodavatelé a dodavatelé budou v přiměřené době vázáni závazky podobným závazkům obsaženým v tomto ustanovení.
6. Na základě žádosti objednatele poskytne dodavatel písemný důkaz o jeho souladu s těmito ustanoveními včetně obecně akceptovatelných zpráv auditorů (např. SSAE-16 SOC 2 Type II).