

## OŚWIADCZENIE WIEDZY

Niżej podpisany działający w imieniu i na rzecz PreZero Service Zachód sp. z o. o. z siedzibą w Kielczu (dalej jako „Spółka”) niniejszym oświadczam, że dokumenty zapisane w wewnętrznym systemie Spółki dotyczące udziału w postępowaniu o udzielenie zamówienia publicznego pod nazwą, ***Sukcesywne usługi odbioru, transportu, unieszkodliwienia odpadów o kodach: 20 03 99, 15 01 01, 15 01 02, 15 01 07, 17 01 01, 20 03 07 i dzierżawy urządzeń do gromadzenia odpadów poszczególnych frakcji („Postępowanie”)*** prowadzone przez Zamawiającego: Szpital Uniwersytecki im. Karola Marcinkowskiego w Zielonej Górze sp. z o. o. nie są dostępne dla wszystkich pracowników oraz współpracowników Spółki.

Z uwagi na szczególny charakter tego zamówienia, dostęp do dokumentów związanych z przygotowaniem oferty, w tym w szczególności, ustaleniem ceny ofertowej i wyjaśnień dotyczących samooczyszczania samooczyszczania związanej z okolicznościami wynikającymi z art. 109 ust. 1 pkt 2c) PZP oraz art. 109 ust. 1 pkt 7) PZP, posiada wyłącznie wąska grupa osób zaangażowanych w Postępowanie z ramienia Spółki. Pozostali pracownicy oraz współpracownicy Spółki, którzy na co dzień mają dostęp do systemu obiegu dokumentów w Spółce, nie posiadają dostępu do dokumentów związanych z Postępowaniem.

Dodatkowo Spółka stosuje fizyczne środki ochrony informacji (ochrona i dozór fizyczny), środki kontroli dostępu do pomieszczeń (zgodnie z nadanymi uprawnieniami), monitoring czy szeroko rozumiane technologie i polityki zapewniające bezpieczeństwo sieci teleinformatycznej:

- a) firewall;
- b) programy antywirusowe;
- c) loginy, hasła wraz z odpowiednią polityką haseł;
- d) globalne oprogramowanie uwierzytelniające tzw. SIAM (Schwarz Identity & Access Management);
- e) szyfrowanie twardych dysków;
- f) Bitlocker;
- g) UTM Sophos;
- h) MFA Office;
- i) MFA VPN, szyfrowany;
- j) stały monitoring działania sieci;
- k) ograniczanie adresacji MAC, tylko dla urządzeń zaufanych (pracownicy);
- l) dostęp do zasobów, systemów ERP, tylko z sieci wewnętrznej i/lub VPN;
- m) reglamentowany dostęp do zasobów sieci zgodnie z zajmowanym stanowiskiem;
- n) zabezpieczenie przeciw instalowaniu nieautoryzowanego oprogramowania;
- o) regularne kampanie phishingowe
- p) szkolenia zwiększające świadomość w obszarze cyberprzestrzeni.

W Spółce funkcjonuje też szereg procedur z zakresu IT i bezpieczeństwa informacji, których celem jest przeciwdziałanie niekontrolowanemu ujawnianiu danych poufnych poza struktury Spółki:

- a) Procedura PR.IT3: Postępowanie z sieciami komputerowymi i technologią;
- b) Procedura PR.IT6: Zarządzanie zdalnym dostępem;
- c) Procedura PR.IT8: Zarządzanie dostępem;
- d) Instrukcja obsługi podwójnej autoryzacji w Microsoft Office/Cloud (MFA);

- e) Instrukcja obsługi zasobów korporacyjnej sieci komputerowej;
- f) Instrukcja konfiguracji i użytkowania VPN.

Powyższe środki bezpieczeństwa są podejmowane w Spółce, aby zapewnić maksymalny zakres ochrony informacji przed ich dostępem osób nieuprawnionych (np. kradzież) czy nieuprawniony dostęp zewnętrzny do sieci teleinformatycznej Spółki.

Z uwagi na powyższe środki bezpieczeństwa oraz stosowane przez Spółkę zabezpieczenia systemów informatycznych, z których korzysta Spółka nie jest możliwe uzyskanie wglądu do dokumentów, o których mowa powyżej, przez jakąkolwiek nieuprawnioną do tego osobę.

Podpis:

---