**Dodatek nr 2 do zapytania**
**Załącznik nr 1 do umowy PCZSzp/ZP/ZO/130/21/2023**

**Wymagania minimalne w zakresie merytorycznych treści szkoleń w zakresie bezpieczeństwa teleinformatycznego**

| l.p. | Minimalny zakres przedmiotu zamówienia |
|---|---|
| 1. | Szkolenia powinny składać się z części teoretycznej i praktycznej oraz szkolenie z SZBI. |
| 2. | Zakres szkolenia w części teoretycznej powinien obejmować tematykę:<br>1. Wycieki danych w ostatnich latach (przykłady) i kary nakładane na administratorów.<br>2. Wyjaśnienie podstawowych pojęć związanych z cyberbezpieczeństwem (https, AES-256, IP, TCP, domena, URL i inne).<br>3. Phishing i ransomware – zasady działania i rozpoznawania tych zagrożeń.<br>4. Wyłudzanie danych osobowych za pomocą technik socjotechnicznych (phishing,/vishing,/smishing/spear phishing) – przykłady z życia urzędów.<br>5. Jak bezpiecznie przetwarzać dane (szyfrowanie, przechowywanie, udostępnianie).<br>6. Zabezpieczenie informatycznych nośników danych – pendrive'y i pamięci zewnętrzne.<br>7. Zasady korzystania z poczty elektronicznej.<br>8. Bezpieczeństwo podczas korzystania z przeglądarek internetowych.<br>9. Bezpieczeństwo danych w chmurze.<br>10. Prywatność w sieci (trakery, ciastka, tryb incognito).<br>11. Bezpieczeństwo pracy zdalnej – jak pracować na sprzęcie własnym oraz służbowym.<br>12. Bezpieczeństwo urządzeń mobilnych.<br>13. Podsumowanie najważniejszych zasad cyberbezpieczeństwa – dobre praktyki/wskazówki. |
| 3. | Zakres szkolenia praktycznego powinien obejmować ćwiczenia praktyczne obejmujące tematykę:<br>1. Rozpoznawanie złośliwego oprogramowania i phishingu.<br>2. Szyfrowanie danych.<br>3. W jaki sposób zabezpieczyć własne dane?<br>4. Rozpoznawanie fałszywych informacji. |
| **4.** | Efektem praktycznego szkolenia, powinno być przekazanie Zamawiającemu wiedzy i umiejętności pozwalających na aktualizację polityki bezpieczeństwa informacji w PCZ Sp. z o.o., w oparciu o aktualne standardy. Wykonawca zobowiązany będzie zweryfikować zaktualizowaną politykę bezpieczeństwa informacji. |
| 5. | Szkolenia z SZBI powinny obejmować tematykę:<br>1. Prawne aspekty bezpieczeństwa informacji i cyberbezpieczeństwa (KRI, UoKSC, rola normy PN ISO/IEC 27001).<br>2. Obowiązki jednostek publicznych w obszarze bezpieczeństwa informacji.<br>3. Odpowiedzialność za naruszenie zasad bezpieczeństwa informacji.<br>4. Procedury wynikające z cyberbezpieczeństwa oraz sposoby ich efektywnego wdrożenia w jednostce.<br>5. Techniki działań uświadamiających oraz zabezpieczających użytkownika wobec cyberzagrożeń.<br>6. Sposoby nadzorowania/audytowania cyberbezpieczeństwa.<br>7. Kompetencje informatyczne celem zachowania bezpieczeństwa informacji:<br>a) bezpieczeństwo sieci LAN i Wi-Fi,<br>b) bezpieczeństwo aplikacji/systemów,<br>c) bezpieczeństwo stacji roboczych (komputery użytkownika),<br>d) zarządzanie tożsamością w internecie oraz wewnątrz organizacji,<br>e) bezpieczeństwo baz danych i infrastruktury,<br>f) bezpieczeństwo w chmurze,<br>g) bezpieczeństwo mobilnym,<br>h) odzyskiwanie po awarii – planowanie ciągłości działania,<br>i) odpowiednie zabezpieczenie techniczne sieci – dla użytkowników,<br>j) bezpieczeństwo podczas pracy zdalnej,<br>k) techniki socjotechniczne. |
| 6. | W oparciu o sprawdzone standardy, Wykonawca przekaże Zamawiającemu szablony poszczególnych polityk, procedur oraz instrukcji jak najbardziej zbliżonych do oczekiwanego, docelowego SZBI Zamawiającego i na ich podstawie przeprowadzi szkolenie. Wykorzystane w trakcie szkolenia materiały (szablony, procedury, instrukcje, przykładowa polityka bezpieczeństwa firmy) po zakończeniu szkolenia pozostaną własnością Zamawiającego. |

| | |
|---|---|
| 7. | Całość działań realizacyjnych ma być zgodna z aktualnym stanem prawnym w zakresie ustawy o Krajowym Systemie Cyberbezpieczeństwa (UoKSC), co najmniej w oparciu o dobre praktyki i wskazania norm:<br>a) PN ISO/IEC 27001 - Systemy zarządzania bezpieczeństwem informacji - Wymagania,<br>b) PN ISO/IEC 27000 - Systemy zarządzania bezpieczeństwem informacji - Przegląd i terminologia,<br>c) PN ISO/IEC 27002 - Praktyczne zasady zabezpieczania informacji,<br>d) PN ISO/IEC 27005 - Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji,<br>e) PN-EN ISO 22301 - Bezpieczeństwo powszechne - Systemy zarządzania ciągłością działania - Wymagania,<br>f) PN-ISO/IEC 20000-1 - Technika informatyczna. Zarządzanie usługami. Część 1: Wymagania dla systemu zarządzania. |