**Część 1 - Dostawa materiałów szkoleniowych z zakresu cyberbezpieczeństwa -załącznik nr 4.1 do SWZ**

**Źródło finansowania zamówienia:** dofinansowanie ze środków UE 81% oraz dofinansowanie z budżetu państwa stanowiące 19% w ramach Projektu grantowego „Cyberbezpieczny Samorząd” współfinansowanego z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Projekt II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa komponentu | Wymagane minimalne parametry techniczne |
| 1. | Informacje ogólne | Zamawiający wymaga dostarczenia minimum 25 lekcji/szkoleń  z zakresu bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego.  Szkolenia dedykowane dla pracowników biurowych pracujących z komputerami i przetwarzających różnego rodzaju informacje o różnym poziomie poufności.  Szkolenia muszą być dostarczone Zamawiającemu w formie gotowego produktu. Zamawiający musi mieć możliwość swobodnego wykorzystania szkoleń bez ograniczeń czasowych oraz liczby odbiorców.  Szkolenia nie mogą być realizowane w formie usługi. |
| 2. | Forma e-learning | Szkolenia muszą być w postaci oddzielnych lekcji.  Jedna lekcja szkolenia powinna zawierać minimum 30 slajdów.  Czas jednej lekcji (tematu) powinien oscylować w granicach 20-30 min.  Lekcje powinny być multimedialne z wykorzystaniem scenek rodzajowych z możliwością odtworzenia w postaci dźwiękowej z użyciem lektora. Nie mogą to być same zdjęcia, definicje lub zagadnienia opisane w formie tekstowej i odtwarzane w postaci dźwiękowej.  Podczas lekcji powinna być na bieżąco weryfikowana wiedza (uwaga) użytkownika poprzez np. ćwiczenia sprawdzające. |
| 3. | Tematyka szkoleń | Szkolenia musza poruszać minimum następujące zagadnienia:   1. Omówienie zagadnień: bezpieczeństwo informacji, zarządzanie bezpieczeństwem. 2. Triada bezpieczeństwa: poufność, dostępność, integralność. 3. Podstawowe informacje odnośnie systemu zarządzania bezpieczeństwem informacji. 4. Internet – zasady bezpiecznego korzystania ze stron www 5. Portale społecznościowe – ryzyka i zagrożenia 6. Poczta elektroniczna – zasady korzystania 7. Hasła i polityki haseł 8. Menedżer haseł 9. Zagrożenia cybernetyczne 10. Phishing – definicja, podstawowe informacje i przykłady 11. Vishing – definicja, podstawowe informacje i przykłady 12. Ransomware – definicja, podstawowe informacje i przykłady 13. Socjotechnika – przykładowe scenariusze ataków socjotechnicznych 14. Muł finansowy – definicja, podstawowe informacje  i przykłady 15. Sposoby korzystania zabezpieczeń i ochrony sieci bezprzewodowych 16. Zasady zabezpieczania sprzętu mobilnego 17. Jak cyberprzestępcy kradną dane przez telefon – definicja, podstawowe informacje i przykłady 18. Prawne aspekty i konsekwencje lekceważenia zasad bezpieczeństwa informacji 19. Płatności elektroniczne – podstawy bezpieczeństwa 20. Zabezpieczenie fizyczne dokumentacji, sprzętu IT  i pomieszczeń 21. Praca zdalna – definicja, podstawowe informacje i przykłady 22. Fake newsy i dezinformacja – definicja, podstawowe informacje i przykłady 23. Cloud – definicja, podstawowe informacje i przykłady 24. Dyrektywa NIS 2 25. AI - definicja, podstawowe informacje |
| 4. | Wymagania techniczne | * Szkolenia w wersji elektronicznej musi być zgodne ze standardem umożliwiającym prezentację na platformie MOODLE w wersji 4.0 lub wyższej. * Szkolenia powinno być dostarczone w technologii HTML5. * Szkolenia powinny być podzielone tematycznie w taki sposób, aby można było operować (zarządzać dostępnością, harmonogramem, itp.) poszczególnymi tematami z osobna. |
| 5. | Forma szkolenia | * Szkolenia muszą posiadać atrakcyjną formę przekazu materiału, zachęcającą osoby uczące się do aktywnego odbywania szkolenia. Zamawiający wymaga atrakcyjnej formy przekazu materiału szkolenia. Atrakcyjna forma to m.in. grafika oparta na scenkach, postaciach, dialogach, przykładach, ćwiczeniach, testach sprawdzających wiedzę oraz dźwięk – głos lektorów powinien być indywidualny dla każdej z postaci występujących w szkoleniu. * Szkolenia muszą posiadać interaktywną formę, zwiększającą zaangażowanie osób uczących się. Szkolenie musi zostać wyposażone w elementy interakcji (np. kliknięcia, ćwiczenia), tak aby uczestnik był aktywny podczas szkolenia i nie miał możliwości zaliczenia szkolenia w sposób bierny tj. poprzez samoczynne odtworzenia filmu/ szkolenia. * Lekcje muszą kłaść duży nacisk na umiejętności praktyczne, nie tylko teorię bezpieczeństwa IT. * Cały materiał szkoleń musi być dostępny w języku polskim i przedstawiony w sposób zrozumiały przez osoby nietechniczne. * Aby szkolenia posiadały wysoką jakość merytoryczną ich scenariusz musiał zostać opracowany we współpracy z ekspertem bezpieczeństwa IT posiadającym certyfikat Lead Auditor 27001. |
| 6. | Licencjonowanie | Licencja musi pozwalać do korzystania ze szkolenia przez nieograniczoną liczbę pracowników w ramach Powiatu. Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na szkolenia. |
| 7. | Gwarancja | 12 miesięcy |