

Załącznik nr 1 do zapytania ofertowego nr RLiOŚ.2710.27.2024

### Opis przedmiotu zamówienia

I. Przedmiotem zamówienia jest przeprowadzenie w Urzędzie Gminy Stanisławów szkoleń z zakresu cyberbezpieczeństwa dla kadry kierowniczej i pracowników Urzędu oraz zakup dostępu do platformy szkoleniowej, na której pracownicy będą mogli na bieżąco szkolić się z zakresu cyberbezpieczeństwa w ramach projektu grantowego „Cyberbezpieczny samorząd”. W ramach projektu przewidziano kompleksowe przeszkolenie i zakup materiałów szkoleniowych z zakresu cyberbezpieczeństwa w celu zapewnienia regularnego podnoszenia poziomu świadomości cyberbezpieczeństwa u wszystkich pracowników.

Przedmiotem zamówienia podzielony jest na 2 części:

część 1 - zakup szkoleń z zakresu cyberbezpieczeństwa dla pracowników IT – specjalistyczne szkolenia dla 2 pracowników IT z zakresu planowanych i zastosowanych środków z zakresu cyberbezpieczeństwa;

część 2 - podniesienie poziomu wiedzy i kompetencji personelu Wnioskodawcy w zakresie cyberbezpieczeństwa:

- a) szkolenie stacjonarne dla kadry kierowniczej,
- b) szkolenie stacjonarne dla pracowników,
- c) dostęp do dedykowanej platformy szkoleniowej dla 30 pracowników.

II. Ocena ofert zostanie przeprowadzona dla każdej części z osobna. Zamawiający nie dopuszcza możliwości składania ofert częściowych.

III. Szkolenia dla części 1 i części 2 lit. a i b muszą spełniać następujące wymagania:

- 1) Miejscem realizacji zamówienia: Urząd Gminy Stanisławów, ul. Rynek 32, 05-304 Stanisławów. Zamawiający może dopuścić zmianę miejsca realizacji szkolenia lub jego formy w przypadku sytuacji nadzwyczajnych (pandemia, klęska żywiołowa, wprowadzenie stanu wyjątkowego, wojny, itp.), uniemożliwiających przeprowadzenie szkolenia stacjonarnego w Urzędzie;
- 2) Szkolenia muszą odbywać się w godzinach pracy Urzędu tj. w poniedziałek od godz. 9.00-17.00, wtorek do piątek w godz. 8.00 – 16.00;
- 3) Wykonawca w ramach wykonania usługi przedstawi szczegółowy program szkolenia zawierający informacje dotyczące tematyki i czasu szkolenia, i dostarczy go w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji Zamawiającego.
- 4) Opracowane materiały będą musiały być dostarczone w formie papierowej i elektronicznej z możliwością powiększania treści. W ramach wynagrodzenia Wykonawca przygotowuje i zapewni materiały szkoleniowe dla każdego uczestnika, pozwalające na samodzielną edukację z zakresu tematyki szkolenia. Zamawiający dopuszcza dostarczenie kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF.
- 5) Wykonawca dostarczy materiały szkoleniowe uczestnikom szkolenia najpóźniej w dniu



rozpoczęcia szkolenia;

6) W ramach wynagrodzenia Wykonawca dostarczy Zamawiającemu materiały ze szkolenia, które to będzie mógł wykorzystać do przeszkolenia osób nieobecnych lub nowoprzyjętych.

7) Wykonawca nie jest zobowiązany do zapewnienia uczestnikom wyżywienia podczas szkoleń stacjonarnych;

8) Każdy uczestnik szkolenia otrzyma od Wykonawcy imienny certyfikat z podpisem trenera, potwierdzający ukończenie szkolenia i jego zakres;

9) Zamawiający zwraca uwagę, że szkolenia będące przedmiotem zamówienia mają charakter kształcenia zawodowego i są finansowane w całości ze środków publicznych, w związku z czym są one zwolnione z podatku od towarów i usług na podstawie §3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 roku w sprawie zwolnień od podatku towarów i usług oraz warunków stosowania tych zwolnień (t.j. Dz.U. 2023 poz. 955).

#### **IV. Szkolenie z Cyberbezpieczeństwa dla pracowników IT.**

W ramach realizacji części 1 zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia specjalistycznego dla informatyka i zastępcy w zakresie zastosowanych, planowanych do zastosowania, środków bezpieczeństwa. Celem szkolenia jest zwiększenie kompetencji pracowników IT w Urzędzie w zakresie nowych zagrożeń i sposobów zapobiegania, przygotowanie ich do skutecznego zabezpieczania systemów informatycznych oraz zarządzania incydentami bezpieczeństwa. Szkolenie ma także za zadanie zwiększenie poziomu ochrony danych oraz zapewnienie zgodności z przepisami prawa.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Podstawy prawne krajowego systemu cyberbezpieczeństwa.
2. Obowiązki wynikające z przepisów rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773) i ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2024 poz. 1077), zapewnienie zgodności działań IT z tymi przepisami.

ocena ryzyka, w tym metody identyfikacji i analizy ryzyka związanego z IT, środki zaradcze w celu minimalizacji ryzyka.

3. Audyt wewnętrzny (cyberbezpieczeństwa) i raportowanie zgodności z przepisami.
4. Zasady postępowania w razie wprowadzenia stopni alarmowych CRP dotyczących zagrożeń w cyberprzestrzeni;
5. Analiza najnowszych zagrożeń cybernetycznych, takich jak ransomware, malware, phishing, ataki DDoS oraz zaawansowane uporczywe zagrożenia (Advanced Persistent Threat – APT), oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania



- pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa i inne metody socjotechniczne,
6. Rozpoznawanie i analiza wzorców ataków i technik stosowanych przez cyberprzestępców oraz sposoby ochrony.
  7. Identyfikacja i klasyfikacja incydentów bezpieczeństwa.
  8. Procedury przyjmowania zgłoszeń incydentów, reagowanie na incydenty.
  9. Sposoby szybkiego reagowania na incydenty oraz koordynacja działań naprawczych;
  10. Szkolenie z zakresu zastosowanych oraz planowanych do zastosowania, środków bezpieczeństwa:
    - 1) Szkolenie z zakresu obsługi urządzeń podwójnego zastosowania:

Konfiguracja Metod Dostępu i Segmentacji Sieci:

      - a) Konfiguracja Metod Dostępu do Urządzeń:
        - Konfiguracja Dostępu SSH i HTTPS:
          - Implementacja i konfiguracja bezpiecznego dostępu do urządzeń.
          - Zarządzanie certyfikatami SSL/TLS.
        - Wdrożenie Dwuetapowej Autoryzacji (2FA):
          - Implementacja 2FA dla zwiększenia bezpieczeństwa dostępu.
          - Konfiguracja aplikacji autoryzujących i tokenów sprzętowych.
      - b) Konfiguracja Łącz Dostępowych do Internetu i Redundancji:
        - Ustawienie Podstawowych Łącz Internetowych:
          - Konfiguracja głównych połączeń internetowych.
          - Monitorowanie i optymalizacja wydajności łączy.
        - Konfiguracja Łącz Zapasowych i Redundancji (WAN):
          - Implementacja zapasowych łączy internetowych.
          - Konfiguracja mechanizmów przełączania awaryjnego i load balancingu.
      - c) Segmentacja Sieci LAN:
        - Konfiguracja Interfejsów Sieciowych:
          - Ustawienia interfejsów fizycznych i logicznych.
          - Optymalizacja parametrów interfejsów dla różnych zastosowań.
        - Konfiguracja VLAN i Polityk Dostępu do Podsieci/VLAN:
          - Tworzenie i zarządzanie VLANami.
          - Implementacja polityk bezpieczeństwa dla poszczególnych VLANów.





## 2) Zarządzanie Siecią i Polityki Bezpieczeństwa:

### a) Uruchomienie Serwerów DHCP:

- Konfiguracja Serwerów DHCP na Poszczególnych Podsieciach/VLAN:
  - Ustawienia serwerów DHCP dla dynamicznego przydzielania adresów IP.
  - Zarządzanie pulami adresów i rezerwacjami.

### b) Konfiguracja Routingu i Agregacji Portów:

- Ustawienia Routingu Statycznego i Dynamicznego:
  - Konfiguracja tras statycznych i protokołów routingu dynamicznego (OSPF, BGP).
  - Optymalizacja trasowania i zarządzanie tablicami routingu.
- Konfiguracja Agregacji Portów dla Zwiększenia Przepustowości:
  - Implementacja agregacji portów (LACP).
  - Balansowanie obciążenia i redundancja portów.

### c) Polityki Bezpieczeństwa:

- Filtrowanie i Blokowanie Treści oraz Aplikacji Internetowych:
  - Konfiguracja filtrów treści i aplikacji.
  - Zarządzanie czarnymi i białymi listami.
- Konfiguracja Antywirusa, Filtrów DNS, IPS i DLP:
  - Implementacja zabezpieczeń antywirusowych i systemów wykrywania intruzji (IPS).
  - Konfiguracja filtrów DNS i polityk zapobiegania wyciekom danych (DLP).
- **Integracja i Zarządzanie Systemem:**

### d) Integracja z Domeną:

- Konfiguracja Urządzeń do Współpracy z Domeną:
  - Procedury integracji z domeną Active Directory.
  - Zarządzanie kontami i politykami bezpieczeństwa domeny.

### e) Konfiguracja SNMP:

- Ustawienia SNMP do Monitorowania Sieci:
  - Konfiguracja protokołu SNMP dla monitorowania i zarządzania urządzeniami sieciowymi.
  - Implementacja pułapek SNMP i zbieranie danych z urządzeń.
- **Logowanie, Kopie Zapasowe i VPN:**

### f) Konfiguracja Procesu Logowania:



- **Konfiguracja Zawartości Logów i Okresu Przechowywania:**
  - Definiowanie typów logów, które mają być przechowywane.
  - Ustalanie okresów retencji logów i zarządzanie przestrzenią dyskową.
- g) **Wykonanie Kopii Zapasowej Ustawień Urządzeń:**
  - **Procedury Tworzenia Kopii Zapasowych i Przywracania Ustawień:**
    - Automatyzacja tworzenia kopii zapasowych ustawień urządzeń.
    - Procedury przywracania ustawień z kopii zapasowych.
- h) **Konfiguracja Tuneli VPN IPsec / SSL:**
  - **Konfiguracja Tuneli VPN Typu IPsec i SSL:**
    - Tworzenie i zarządzanie tunelami VPN dla bezpiecznej komunikacji.
    - Konfiguracja polityk bezpieczeństwa VPN i zarządzanie certyfikatami.

## 11. Szkolenie z zakresu Microsoft Windows Server

- 1) Instalacja Active Directory na Microsoft Windows Server.
- 2) Dodawanie drugiego kontrolera do AD
- 3) Podstawowe narzędzia do zarządzania Active Directory
- 4) Zarządzanie użytkownikami:
  - Dodawanie nowych użytkowników
  - Właściwości obiektu użytkownika
  - Grupy użytkowników
  - Zarządzanie uprawnieniami użytkowników
- 5) Rola DNS w Active Directory.
- 6) Dodawanie komputerów do Active Directory:
- 7) Polityki grup:
  - Stosowanie polityk grup do zabezpieczania Active Directory
  - Dane na serwerze - przekierowanie folderów
  - Instalacja oprogramowania przy pomocy GPO
- 8) Dodawanie kolejnych kontrolerów do domeny Active Directory - redundancja:
  - Przenoszenie ról FSMO
- 9) Windows Server Backup
- 10) Firewall w systemie Windows Server:
  - Dodawanie i edycja reguł firewalla



- 11) Network Policy Server (RADIUS) i jego integracja z Active Directory
  - 12) Active Directory Certificate Services
  - 13) Konfiguracja serwerów pracujących w systemie operacyjnym Windows Server w klastrze.
12. Szkolenia muszą obejmować ćwiczenia praktyczne – min. 30% czasu trwania szkolenia.
  13. Wymagana forma przeprowadzenia szkolenia: szkolenie stacjonarne indywidualne. Zamawiający zapewni pomieszczenie i komputer do przeprowadzenia szkolenia.
  14. Czas trwania szkolenia 16 godzin lekcyjnych po 45.min.
  15. Z przeprowadzonych szkoleń Wykonawca musi przedstawić potwierdzenie realizacji szkolenia z podpisem uczestnika.
  16. Szkolenia muszą być prowadzone osoby posiadające doświadczenie wymienione w zapytaniu ofertowym oraz przez jednego certyfikowanego inżyniera, posiadającego minimum 3 aktywne certyfikaty:
    - Certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci(NS)
    - Certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa(SO)
    - Certyfikowany Specjalista w zakresie Dostępu Zero Trust(ZTA)

## **V. Szkolenie stacjonarne dla pracowników i kadry kierowniczej**

1. W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia podstawowego szkolenia stacjonarnego dla pracowników Urzędu Gminy oraz kadry zarządzającej budującego świadomość cyberzagrożeń i sposobów ochrony JST. Szkolenie musi zbudować świadomość i umiejętności praktyczne pracowników Urzędu w zakresie cyberzagrożeń i sposobów ochrony przed nimi oraz problematyki związanej z bezpieczeństwem informacji, w tym z codziennym zabezpieczaniem danych i reagowaniem na zagrożenia.
2. Szkolenie musi obejmować co najmniej następującą tematykę:
  - 1) podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania),
  - 2) cyberbezpieczeństwo w codziennej pracy urzędu,
  - 3) Zagrożenia dla bezpieczeństwa danych:
    - Przechwycenie przez niepowołane osoby (dane w transmisji, dane "w spoczynku")
    - Utrata danych i utrata dostępu do danych w wyniku ataku (włamanie, wirus, trojan, ransomware)
    - Utrata danych i utrata dostępu do danych w wyniku awarii (przerwa w zasilaniu, awaria urządzeń, awaria nośników)
    - Utrata dostępu do danych w wyniku utraty danych uwierzytelniających.
    - Straty wynikające z naruszenia bezpieczeństwa danych.
  - 4) Zabezpieczenie danych przed przechwyceniem przez niepowołane osoby lub ich utratą w wyniku ataku:





- Szyfrowanie danych (w transmisji, w spoczynku),
- Bezpieczeństwo sieci lokalnej (kontrola dostępu do sieci przewodowej, DMZ, odseparowanie WiFi)
- Ograniczanie dostępu do udostępnianych danych (udostępnianie wybranych zasobów, dostęp dla określonych użytkowników),
- Ochrona przed włamaniem,
- Silne hasła,
- Ochrona haseł i kluczy - dobre praktyki,
- Uwierzytelnianie dwuskładnikowe, biometryczne, przy pomocy certyfikatu,
- Korzystanie z poczty elektronicznej - dobre praktyki w zakresie ochrony przed phishingiem i malware,
- Oprogramowanie antywirusowe / chroniące komputer,
- Aktualizacje systemu i oprogramowania,
- Nieużywanie nieautoryzowanego oprogramowania,
- Nie daj się podejść oszustowi,
- Fizyczne zabezpieczenia danych (dostęp do urządzeń, nośników, pomieszczeń, procedury postępowania z niewykorzystywanymi już nośnikami, zasada "czystego biurka"),
- Procedury dotyczące używania urządzeń prywatnych (praca zdalna, BYOD).

5) Zabezpieczenie danych przed utratą:

- Prewencyjna ochrona przed utratą danych w wyniku zaniku zasilania (UPS, sprawne baterie w laptopach, redundancja zasilania). Prewencyjna ochrona przed utratą danych lub dostępu do danych w wyniku innej awarii (konserwacja sprzętu, redundancja urządzeń / klastry, umowy serwisowe)
- Kopie zapasowe;

6) Zabezpieczenie danych przed utratą dostępu w wyniku utraty danych uwierzytelniających:

- Dostęp administracyjny (zapasowe konta administracyjne, wielość administratorów, umowy),
- Przechowywanie haseł.

3. Szkolenia mają obejmować ćwiczenia praktyczne (min. 20% czasu trwania szkolenia), pozwalające na podniesienie umiejętności związanych z:

- rozpoznawaniem zagrożeń i reagowanie na nie,



- wykorzystywaniem narzędzi informatycznych zapewniających bezpieczeństwo przetwarzanych informacji oraz zabezpieczeń dla poczty elektronicznej i stron WWW
  - radzeniem sobie w sytuacjach kryzysowych (scenariusze codziennych zagrożeń).
4. W trakcie szkolenia trener powinien odpowiadać na pytania uczestników. Dopuszczalne jest zorganizowanie sesji pytań i odpowiedzi na zakończenie szkolenia.
  5. W wyniku szkolenia pracownicy mają być w stanie odróżnić typowe błędy techniczne od potencjalnego ataku, wiedzieć jak uniknąć potencjalnego zagrożenia, a w przypadku wystąpienia naruszenia – umieć podjąć podstawowe działania ograniczające skutki wystąpienia incydentu oraz zgłosić incydent do odpowiednich komórek.
  6. Wymagana forma przeprowadzenia szkolenia: szkolenie stacjonarne. Zamawiający zapewni salę szkoleniową na maksymalnie 20 osób z ekranem, rzutnikiem.
  7. Łączna liczba osób do przeszkolenia 30 z podziałem na dwie grupy pracowników – 24 osobu i 6 osób kadry kierowniczej. (maksymalnie 20 osób w grupie)
  8. Czas trwania szkolenia dla każdej z grup – min. 8 godzin lekcyjnych (po 45 min.).
  9. Program szkolenia powinien zostać zmodyfikowany i powinien różnić dla pracowników i dla kadry kierowniczej.
  10. Z przeprowadzonych szkoleń Wykonawca musi przedstawić listy obecności z podpisami uczestników szkolenia.
  11. Każdy uczestnik szkolenia otrzyma od Wykonawcy imienny certyfikat z podpisem trenera, potwierdzający ukończenie szkolenia i jego zakres;
  12. Zamawiający zwraca uwagę, że szkolenia będące przedmiotem zamówienia mają charakter kształcenia zawodowego i są finansowane w całości ze środków publicznych, w związku z czym są one zwolnione z podatku od towarów i usług na podstawie §3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 roku w sprawie zwolnień od podatku towarów i usług oraz warunków stosowania tych zwolnień (t.j. Dz.U. 2023 poz. 955).
  13. Wykonawca musi zatrudniać co najmniej jedną osobę z aktualnym certyfikatem: CISSP oraz CEH.

## **VI. Dostawa platformy szkoleniowej dla pracowników Urzędu**

1. W ramach realizacji zamówienia Wykonawca zobowiązany będzie do zapewnienia kompleksowej usługi „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness), umożliwiającej przeprowadzenie kampanii edukacyjnej z zakresu podstaw cyberbezpieczeństwa. Dedykowanej 30 użytkownikom Zamawiającego i świadczonej przez okres 12 miesięcy
2. Usługa musi zawierać:
  - 1) Platformę szkoleniową zawierającą minimum 50 szkoleń, dostępnych w języku polskim oraz w jęz. angielskim, w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.
- a) Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:



- ✓ Podstawy bezpiecznego internetu,
- ✓ Bezpieczeństwo poczty,
- ✓ Załączników w poczcie elektronicznej,
- ✓ Phishing,
- ✓ Spyware/malware,
- ✓ Bezpieczeństwo danych osobowych RODO/GDPR,
- ✓ Bezpieczne hasła,
- ✓ Menedżery haseł,
- ✓ Bezpieczeństwo urządzeń mobilnych,
- ✓ Uwierzytelnianie wieloskładnikowe (MFA),
- ✓ Bezpieczna praca zdalna,
- ✓ Bezpieczna praca w biurze,
- ✓ Sieci społeczne,
- ✓ Socjotechnika stosowana,
- ✓ Zakupy w internecie,

b) Platforma powinna umożliwić Zamawiającemu dokonania podziału Użytkowników na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.

c) Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 8 godzin.

2) Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:

a) z linkiem prowadzącym do stronnym internetowej,

b) z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,

c) z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,

d) z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.

W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.

3) dedykowaną platformę dostarczającą raporty obejmujące minimum:

- a) status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,



b) status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zawierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.

3. W ramach świadczonej usługi usługodawca musi:

- przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,
- zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,
- zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
- dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,
- wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników (nie więcej niż 10 zmian w okresie trwania usługi).

4. Platforma musi spełniać następujące wymagania:

- 1) działać w przeglądarkach internetowych (Microsoft Edge, Mozilla Firefox i Google Chrome), bez konieczności instalowania dodatkowych komponentów po stronie klienta,
- 2) mieć interfejs użytkownika w języku polskim,
- 3) umożliwiać jednoznaczne zidentyfikowanie i uwierzytelnienie użytkownika za pomocą unikalnego loginu i hasła,
- 4) być dostosowana do potrzeb osób z niepełnosprawnościami zgodnie ze standardami WCAG 2.1 (w tym osobna wersja kontrastowa – przełączanie co najmniej na stronie startowej),
- 5) nowe lub zaktualizowane materiały szkoleniowe muszą być oznaczone jako „nowe”,
- 6) umożliwiać zalogowanemu użytkownikowi pełen dostęp do wszystkich materiałów szkoleniowych i nieograniczony czas na zapoznanie się z materiałami szkoleniowymi przez cały czas dostępu do platformy,
- 7) umożliwiać sprawdzenie nabytej wiedzy za pomocą testów nieograniczonych czasem i liczbą podejść (dotyczy każdego z modułu szkoleniowych z osobna) – dla każdego testu określa się próg zaliczenia – ile % poprawnych odpowiedzi pozwala na zdanie testu,
- 8) testy muszą zawierać znacznik pokazujący w którym miejscu testu użytkownik się znajduje i ile kroków zostało do końca (liczbowo, np. pytanie 7 z 30, lub procentowo),
- 9) po zakończeniu testu użytkownik musi mieć możliwość sprawdzenia swoich odpowiedzi i porównania ich z poprawnymi – poprawne odpowiedzi powinny być opatrzone komentarzem wyjaśniającym dlaczego właśnie ta odpowiedź jest poprawna,
- 10) umożliwiać pobranie imiennego certyfikatu z wynikami po pozytywnym zaliczeniu testu,



- 11) zapamiętywać dla każdego użytkownika postęp szkolenia poprzez oznaczenie materiałów jako przeglądane lub nie oraz rozpoczętych i zaliczonych testów,
- 12) posiadać panel administracyjny, w którym uprawniony użytkownik może przeglądać postępy indywidualne każdego z pozostałych użytkowników,
- 13) w panelu administracyjnym, uprawniony użytkownik może wygenerować raporty zbiorcze dla każdego użytkownika, każdego szkolenia, oraz dla wszystkich użytkowników wraz ze szczegółami dotyczącymi postępów i wyników testów.

Zamawiający zastrzega sobie prawo weryfikacji, czy realizowana usługa spełnia wszystkie określone powyżej wymagania.

Wykonawca dostarczy Zamawiającemu 2 raporty zbiorcze dla każdego użytkownika, każdego szkolenia, oraz dla wszystkich użytkowników wraz ze szczegółami dotyczącymi postępów i wyników testów po 6 miesiącach i na koniec dostępu do platformy. Raporty zostaną dostarczone w postaci elektronicznej wraz z podsumowaniem.

#### Wymagania dodatkowe:

- 1) Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.
- 2) Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.
- 3) Do oferty należy załączyć oświadczenie usługodawcy o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001.

