Załącznik nr 2
do ZO.7031.21.2025.IT

Znak sprawy: **ZO.7031.21.2025.IT**

OPIS PRZEDMIOTU ZAMÓWIENIA

Dla zadania pn.: **„Przeprowadzenie szkoleń dla kadry kierowniczej, pracowników Urzędu Miejskiego w Aleksandrowie Kujawskim i jednostek organizacyjnych Gminy Miejskiej w ramach realizacji projektu pn. „Cyberbezpieczny Samorząd – Wzmocnienie systemu cyberbezpieczeństwa w Gminie Miejskiej Aleksandrów Kujawski"**

Przedmiotem zamówienia jest przeprowadzenie szkoleń dla kadry kierowniczej, pracowników Urzędu Miejskiego w Aleksandrowie Kujawskim i jednostek organizacyjnych Gminy Miejskiej. Przedmiot zamówienia podzielony jest na **9 części.** Ocena ofert zostanie przeprowadzona odrębnie dla każdej części. Niniejszy dokument określa opis przedmiotu zamówienia z minimalnymi wymaganiami dla Zamawiającego. Wykonawca musi wykazać, że oferuje przedmiot zamówienia w pełni zgodny z wymaganym przez Zamawiającego.

Opis zasad warunków równoważności:

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne.
5. Brak określenia „minimum" oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne

uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.

7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. W tym przypadku należy do postępowania dołączyć wszelkie dowody wskazujące na spełnienie niniejszych wymagań.

Opis przedmiotu zamówienia dla poszczególnych jego części:

Część 1: Podstawowe szkolenie stacjonarne budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników Urzędu Miejskiego w Aleksandrowie Kujawskim w 2025 r.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia **stacjonarnego** szkolenia w **2 grupach**, przy czym szkolenia tych grup nie mogą trwać jednocześnie, aby nie powodować utrudnień w ciągłości pracy danej Jednostki. W szkoleniu udział będzie brało około **40 pracowników**. Szkolenie dla jednej grupy powinno trwać minimum 3 godziny zegarowe (łącznie z przerwami), powinno odbyć się w dni robocze, w godzinach pracy Urzędu Miejskiego w miejscu wskazanym przez Zamawiającego.

Wszystkie opracowane materiały szkoleniowe, certyfikaty, zaświadczenia muszą zawierać informację o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu „Cyberbezpieczny samorząd” oraz logotypy.

Zamawiający wymaga realizacji szkoleń według szczegółowego programu zawierającego informacje dotyczące tematyki i czasu szkolenia opracowanego przez Wykonawcę oraz dostarczonego Zamawiającemu na co najmniej 7 dni przed rozpoczęciem szkolenia. Zamawiający zastrzega sobie prawo wniesienia uwag do przedłożonego programu.

Celem szkolenia jest podniesienie świadomości wszystkich pracowników Urzędu w zakresie zagrożeń cyberbezpieczeństwa, sposobów ochrony informacji, zgodnie z najnowszymi zaleceniami jak również zrozumienie przepisów prawnych.
Szkolenie musi obejmować co najmniej następującą tematykę:

1. Podstawy cyberbezpieczeństwa – podstawowe pojęcia i zasady działania.
2. Znaczenie cyberbezpieczeństwa dla jednostki samorządu terytorialnego.
3. Przegląd najpopularniejszych zagrożeń oraz ataków w cyberprzestrzeni.
4. Zagrożenia cybernetyczne i sposoby ochrony, takie jak zagrożenia związane z korzystaniem z internetu, z pocztą elektroniczną, z urządzeniami mobilnymi, z pracą zdalną.
5. Praktyczne zasady bezpieczeństwa, w tym metody codziennej ochrony informacji. Bezpieczne korzystanie z poczty elektronicznej, stron internetowych. urządzeń mobilnych, bezpieczna praca zdalna, zasada czystego biurka i ekranu.
6. Bezpieczeństwo w organizacji. Obowiązki jednostek publicznych wynikające z aktualnego stanu prawnego w obszarze bezpieczeństwa informacji - KRI – Krajowe Ramy Interoperacyjności.
7. Składowe systemu zarządzania bezpieczeństwem informacji oraz zasady bezpieczeństwa informacji.
8. Ochrona danych osobowych.
9. Szyfrowanie dokumentów w ramach dostępnych funkcji.
10. Reagowanie na incydenty bezpieczeństwa.
11. Sesja pytań i odpowiedzi.

Część 2: Podstawowe szkolenie stacjonarne budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników Urzędu Miejskiego w Aleksandrowie Kujawskim w 2026 r.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia **stacjonarnego** szkolenia w **2 grupach**, przy czym szkolenia tych grup nie mogą trwać jednocześnie, aby nie powodować utrudnień w ciągłości pracy danej Jednostki. W szkoleniu udział będzie brało około **40 pracowników**. Szkolenie dla jednej grupy powinno trwać minimum 3 godziny zegarowe (łącznie z przerwami), powinno odbyć się w dni robocze, w godzinach pracy Urzędu Miejskiego w miejscu wskazanym przez Zamawiającego.

Wszystkie opracowane materiały szkoleniowe, certyfikaty, zaświadczenia, programy muszą zawierać informację o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu „Cyberbezpieczny samorząd” oraz logotypy.

Zamawiający wymaga realizacji szkoleń według szczegółowego programu zawierającego informacje dotyczące tematyki i czasu szkolenia opracowanego przez Wykonawcę oraz

dostarczonego Zamawiającemu na co najmniej 7 dni przed rozpoczęciem szkolenia. Zamawiający zastrzega sobie prawo wniesienia uwag do przedłożonego programu.

Celem szkolenia jest podniesienie świadomości wszystkich pracowników Urzędu w zakresie zagrożeń cyberbezpieczeństwa, sposobów ochrony informacji, zgodnie z najnowszymi zaleceniami jak również zrozumienie przepisów prawnych.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Podstawy cyberbezpieczeństwa – podstawowe pojęcia i zasady działania.
2. Znaczenie cyberbezpieczeństwa dla jednostki samorządu terytorialnego.
3. Przegląd najpopularniejszych zagrożeń oraz ataków w cyberprzestrzeni.
4. Zagrożenia cybernetyczne i sposoby ochrony, takie jak zagrożenia związane z korzystaniem z internetu, z pocztą elektroniczną, z urządzeniami mobilnymi, z pracą zdalną.
5. Praktyczne zasady bezpieczeństwa, w tym metody codziennej ochrony informacji. Bezpieczne korzystanie z poczty elektronicznej, stron internetowych. urządzeń mobilnych, bezpieczna praca zdalna, zasada czystego biurka i ekranu.
6. Bezpieczeństwo w organizacji. Obowiązki jednostek publicznych wynikające z aktualnego stanu prawnego w obszarze bezpieczeństwa informacji - KRI – Krajowe Ramy Interoperacyjności.
7. Składowe systemu zarządzania bezpieczeństwem informacji oraz zasady bezpieczeństwa informacji.
8. Ochrona danych osobowych.
9. Szyfrowanie dokumentów w ramach dostępnych funkcji.
10. Reagowanie na incydenty bezpieczeństwa.
11. Sesja pytań i odpowiedzi.

Część 3: Szkolenie z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji dla pracowników Urzędu Urzędu Miejskiego w Aleksandrowie Kujawskim w 2025 r.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia **stacjonarnego** szkolenia **w 2 grupach**, przy czym szkolenia tych grup nie mogą trwać jednocześnie, aby nie powodować utrudnień w ciągłości pracy danej Jednostki. W szkoleniu udział będzie brało **4 pracowników**. Szkolenie dla jednej grupy powinno trwać minimum 3 godziny zegarowe (łącznie z przerwami), powinno odbyć się w dni robocze, w godzinach pracy Urzędu Miejskiego w miejscu wskazanym przez Zamawiającego.

Wszystkie opracowane materiały szkoleniowe, certyfikaty, zaświadczenia, programy muszą zawierać informację o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu

„Cyberbezpieczny samorząd” oraz logotypy.

Zamawiający wymaga realizacji szkoleń według szczegółowego programu zawierającego informacje dotyczące tematyki i czasu szkolenia opracowanego przez Wykonawcę oraz dostarczonego Zamawiającemu na co najmniej 7 dni przed rozpoczęciem szkolenia. Zamawiający zastrzega sobie prawo wniesienia uwag do przedłożonego programu.

Celem szkolenia jest podniesienie świadomości kadry kierowniczej Urzędu w zakresie zagrożeń cyberbezpieczeństwa. Kadra kierownicza musi być w stanie efektywnie zarządzać cyberbezpieczeństwem w urzędzie, podejmować strategiczne decyzje dotyczące ochrony danych oraz promować kulturę bezpieczeństwa wśród pracowników. Dzięki temu Urząd będzie lepiej przygotowany na ewentualne zagrożenia i incydenty.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Rola i obowiązki kadry kierowniczej w zakresie cyberbezpieczeństwa wynikające z aktów prawnych i wdrożonych polityk.
2. Organy i instytucje zwalczające zagrożenia w cyberprzestrzeni.
3. Zasady postępowania w razie wprowadzenia stopni alarmowych CRP dotyczących zagrożeń w cyberprzestrzeni.
4. Cyberbezpieczeństwo jednostki samorządu terytorialnego w kontekście bezpieczeństwa państwa.
5. Obowiązki jednostek samorządu terytorialnego wynikające z przepisów.
6. Standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w urzędzie, cyberhigiena.
7. Procesy i procedury zarządzania incydentami oraz role poszczególnych pracowników.
8. Rola kadry kierowniczej w zakresie cyberbezpieczeństwa (w tym w sytuacjach kryzysowych).
9. Incydenty w kontekście zachowania ciągłości działania urzędu.
10. Przywództwo, motywowanie zespołu i promocja kultury bezpieczeństwa w urzędzie.
11. Sesja pytań i odpowiedzi.

Część 4: Szkolenie z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji dla pracowników Urzędu Urzędu Miejskiego w Aleksandrowie Kujawskim w 2026 r.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia **stacjonarnego** szkolenia w **2 grupach**, przy czym szkolenia tych grup nie mogą trwać jednocześnie, aby nie powodować utrudnień w ciągłości pracy danej Jednostki. W szkoleniu udział będzie brało **4 pracowników**. Szkolenie dla jednej grupy powinno trwać minimum 3 godziny zegarowe (łącznie z przerwami), powinno odbyć się w dni robocze, w godzinach pracy Urzędu

Miejskiego w miejscu wskazanym przez Zamawiającego.

Wszystkie opracowane materiały szkoleniowe, certyfikaty, zaświadczenia, programy muszą zawierać informację o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu „Cyberbezpieczny samorząd” oraz logotypy.

Zamawiający wymaga realizacji szkoleń według szczegółowego programu zawierającego informacje dotyczące tematyki i czasu szkolenia opracowanego przez Wykonawcę oraz dostarczonego Zamawiającemu na co najmniej 7 dni przed rozpoczęciem szkolenia. Zamawiający zastrzega sobie prawo wniesienia uwag do przedłożonego programu.

Celem szkolenia jest podniesienie świadomości kadry kierowniczej Urzędu w zakresie zagrożeń cyberbezpieczeństwa. Kadra kierownicza musi być w stanie efektywnie zarządzać cyberbezpieczeństwem w urzędzie, podejmować strategiczne decyzje dotyczące ochrony danych oraz promować kulturę bezpieczeństwa wśród pracowników. Dzięki temu Urząd będzie lepiej przygotowany na ewentualne zagrożenia i incydenty.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Rola i obowiązki kadry kierowniczej w zakresie cyberbezpieczeństwa wynikające z aktów prawnych i wdrożonych polityk.
2. Organy i instytucje zwalczające zagrożenia w cyberprzestrzeni.
3. Zasady postępowania w razie wprowadzenia stopni alarmowych CRP dotyczących zagrożeń w cyberprzestrzeni.
4. Cyberbezpieczeństwo jednostki samorządu terytorialnego w kontekście bezpieczeństwa państwa.
5. Obowiązki jednostek samorządu terytorialnego wynikające z przepisów.
6. Standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w urzędzie, cyberhigiena.
7. Procesy i procedury zarządzania incydentami oraz role poszczególnych pracowników.
8. Rola kadry kierowniczej w zakresie cyberbezpieczeństwa (w tym w sytuacjach kryzysowych).
9. Incydenty w kontekście zachowania ciągłości działania urzędu.
10. Przywództwo, motywowanie zespołu i promocja kultury bezpieczeństwa w urzędzie.
11. Sesja pytań i odpowiedzi.

Część 5: Dostęp do platformy szkoleniowej dla pracowników Jednostek Podległych Gminy Miejskiej w Aleksandrowie Kujawskim.

Zamawiający chce zakupić usługę podstawowych szkoleń pracowników jednostek podległych w zakresie cyberbezpieczeństwa realizowanych w formie dostępu do platformy szkoleniowej. Usługa ma obejmować dostęp dla 140 kont w okresie od dnia podpisania umowy do dnia **29.05.2026 r.** - wymóg wynikający z obwarowań projektowych. Szkolenia dostępne on-line,

a realizowane przez pracowników za pomocą stacji roboczej. Szkolenie powinno kończyć się sprawdzeniem wiedzy i przy pozytywnym rezultacie wystawieniem imiennego certyfikatu/zaświadczenia. Po upływie maksymalnego terminu realizacji szkolenia Zamawiający otrzyma opis ile osób przystąpiło do szkolenia oraz ile osób zaliczyło sprawdzenie wiedzy.

Materiały szkoleniowe muszą być przez Wykonawcę na bieżąco uzupełniane i aktualizowane w związku z pojawieniem się nowych zagrożeń i podatności, nowych metod ochrony informacji i narzędzi do tego wykorzystywanych oraz zmieniającej się sytuacji geopolitycznej.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Podstawy cyberbezpieczeństwa – podstawowe pojęcia i zasady działania.
2. Znaczenie cyberbezpieczeństwa dla jednostki samorządu terytorialnego.
3. Przegląd najpopularniejszych zagrożeń oraz ataków w cyberprzestrzeni.
4. Zagrożenia cybernetyczne i sposoby ochrony, takie jak zagrożenia związane z korzystaniem z internetu, z pocztą elektroniczną, z urządzeniami mobilnymi, z pracą zdalną.
5. Praktyczne zasady bezpieczeństwa, w tym metody codziennej ochrony informacji. Bezpieczne korzystanie z poczty elektronicznej, stron internetowych. urządzeń mobilnych, bezpieczna praca zdalna, zasada czystego biurka i ekranu.
6. Bezpieczeństwo w organizacji.
7. Reagowanie na incydenty bezpieczeństwa.
8. Składowe systemu zarządzania bezpieczeństwem informacji oraz zasady bezpieczeństwa informacji.
9. Ochrona danych osobowych.
10. Szyfrowanie dokumentów w ramach dostępnych funkcji.
11. Socjotechnika, przykłady zastosowania.
12. Zapewnienie możliwości zamieszczania przez Zamawiającego własnych materiałów szkoleniowych.

Część 6: Szkolenie specjalistyczne dla kadry kierowniczej w zakresie zastosowanych środków bezpieczeństwa.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia **stacjonarnego** szkolenia specjalistycznego **dla 1 osoby** z kadry kierowniczej Urzędu. Szkolenie powinno trwać minimum 3 godziny zegarowe (łącznie z przerwami), powinno odbyć się w dni robocze, w godzinach pracy Urzędu Miejskiego w miejscu wskazanym przez Zamawiającego.

Wszystkie opracowane materiały szkoleniowe, certyfikaty, zaświadczenia, programy muszą zawierać informację o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu „Cyberbezpieczny samorząd” oraz logotypy.

Zamawiający wymaga realizacji szkoleń według szczegółowego programu zawierającego informacje dotyczące tematyki i czasu szkolenia opracowanego przez Wykonawcę oraz dostarczonego Zamawiającemu na co najmniej 7 dni przed rozpoczęciem szkolenia. Zamawiający zastrzega sobie prawo wniesienia uwag do przedłożonego programu.

Celem szkolenia jest podniesienie wiedzy oraz kompetencji kadry kierowniczej Urzędu w zakresie zastosowanych oraz planowanych do zastosowania środków bezpieczeństwa. Dzięki temu Urząd będzie lepiej przygotowany na ewentualne zagrożenia i incydenty.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Wpływ NIS2 na cyberbezpieczeństwo w Urzędzie.
2. Ocena ryzyka, w tym metody identyfikacji i analizy ryzyka związanego z IT, środki zaradcze w celu minimalizacji ryzyka.
3. Rozpoznawanie i analiza wzorców ataków i technik stosowanych przez cyberprzestępców oraz sposoby ochrony.
4. Identyfikacja i klasyfikacja incydentów bezpieczeństwa.
5. Procedury przyjmowania zgłoszeń incydentów, reagowanie na incydenty.
6. Sposoby szybkiego reagowania na incydenty oraz koordynacja działań naprawczych.
7. Tworzenie planu zarządzania ryzykiem.
8. Wyznaczenie zagrożeń i analiza ryzyka w sieci oraz dla procesu uwierzytelniania.
9. Bezpieczeństwo i ochrona danych, w tym mechanizmy ochrony danych, takie jak szyfrowanie i tworzenie kopii zapasowych, zrozumienie zasad ochrony danych osobowych zgodnie z RODO,
10. Umiejętność skutecznej komunikacji z zespołem, z innymi komórkami urzędu i jednostek podległych oraz z interesariuszami zewnętrznymi w sprawach cyberbezpieczeństwa.
11. Profilaktyka cyberbezpieczeństwa w urzędzie, standardy i najlepsze praktyki w tym w zakresie bezpieczeństwa urządzeń i bezpieczeństwa fizycznego.

Część 7: Szkolenia specjalistyczne dla informatyków w zakresie zastosowanych środków bezpieczeństwa.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia specjalistycznego **dla 3 osób** – informatyków Urzędu w formule **on-line**. Szkolenie powinno trwać minimum 3 godziny zegarowe (łącznie z przerwami).

Szkolenie musi obejmować ilość ćwiczeń praktycznych (min. 30% czasu trwania szkolenia), pozwalających na zwiększenie kompetencji kadry kierowniczej w urzędzie związanych z:

1. symulacjami incydentów bezpieczeństwa,
2. analizą rzeczywistych przypadków naruszeń bezpieczeństwa,
3. zarządzaniem w sytuacjach kryzysowych.

Wszystkie opracowane materiały szkoleniowe, certyfikaty, zaświadczenia, programy muszą

zawierać informację o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu „Cyberbezpieczny samorząd” oraz logotypy.

Zamawiający wymaga realizacji szkoleń według szczegółowego programu zawierającego informacje dotyczące tematyki i czasu szkolenia opracowanego przez Wykonawcę oraz dostarczonego Zamawiającemu na co najmniej 7 dni przed rozpoczęciem szkolenia. Zamawiający zastrzega sobie prawo wniesienia uwag do przedłożonego programu.

Celem szkolenia jest podniesienie wiedzy oraz kompetencji informatyków Urzędu w zakresie zastosowanych oraz planowanych do zastosowania środków bezpieczeństwa. Dzięki temu Urząd będzie lepiej przygotowany na ewentualne zagrożenia i incydenty.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Wpływ NIS2 na cyberbezpieczeństwo w Urzędzie.
2. Ocena ryzyka, w tym metody identyfikacji i analizy ryzyka związanego z IT, środki zaradcze w celu minimalizacji ryzyka.
3. Rozpoznawanie i analiza wzorców ataków i technik stosowanych przez cyberprzestępców oraz sposoby ochrony.
4. Identyfikacja i klasyfikacja incydentów bezpieczeństwa.
5. Procedury przyjmowania zgłoszeń incydentów, reagowanie na incydenty.
6. Sposoby szybkiego reagowania na incydenty oraz koordynacja działań naprawczych.
7. Wyznaczenie zagrożeń i analiza ryzyka w sieci oraz dla procesu uwierzytelniania.
8. Sposoby wykorzystania kryptografii do zabezpieczania informacji.
9. Metody szyfrowania.
10. Zabezpieczanie informacji w organizacji przy użyciu uwierzytelniania oraz kontroli dostępu.
11. Bezpieczeństwo i ochrona danych, w tym mechanizmy ochrony danych, takie jak szyfrowanie i tworzenie kopii zapasowych, zrozumienie zasad ochrony danych osobowych zgodnie z RODO,
12. Profilaktyka cyberbezpieczeństwa w urzędzie, standardy i najlepsze praktyki w tym w zakresie bezpieczeństwa urządzeń i bezpieczeństwa fizycznego.

Część 8: Szkolenia specjalistyczne w zakresie audytora ISO IEC 27001 dla 2 osób Urzędu Miejskiego.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia specjalistycznego **dla 3 osób** – informatyków Urzędu w formule on-line w zakresie audytora wewnętrznego ISO/IEC 27001. Celem szkolenia jest zrozumienie wymagań i wytycznych ISO IEC 27001, zdobycie wiedzy praktycznej w oparciu o system zarządzania bezpieczeństwem informacji. Szkolenie powinno zakończyć się uzyskaniem przez pracownika **certyfikatu** ukończenia szkolenia z akredytacją Polskiego Centrum Akredytacji..

Ostateczna cena szkolenia skalkulowana dla 3 osób musi zawierać koszt przeprowadzenia szkolenia, w tym koszt materiałów szkoleniowych i wydanie zaświadczeń o jego ukończeniu, koszt przeprowadzenia procesu certyfikacji, obejmujący egzamin kończący się uzyskaniem oraz wydaniem certyfikatu.

Wszystkie opracowane materiały szkoleniowe, certyfikaty, zaświadczenia, programy muszą zawierać informację o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu „Cyberbezpieczny samorząd" oraz logotypy.

Zamawiający wymaga realizacji szkoleń według szczegółowego programu zawierającego informacje dotyczące tematyki i czasu szkolenia opracowanego przez Wykonawcę oraz dostarczonego Zamawiającemu na co najmniej 7 dni przed rozpoczęciem szkolenia. Zamawiający zastrzega sobie prawo wniesienia uwag do przedłożonego programu.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Zapoznanie z wymaganiami normy ISO/IEC 27001:2022 (norma ta jest tożsama z PN-EN ISO/IEC 27001:2023).
2. Podstawy audytowania.
3. Metody i techniki audytowania – planowanie i przeprowadzanie audytu.
4. Podejście procesowe do ochrony informacji i bezpieczeństwa systemów informatycznych
5. Ustanowienie, rozwój i utrzymanie systemów informacyjnych.
6. Podstawowe pojęcia dotyczące urządzeń, systemów i sieci informacyjnych - analiza i ocena ryzyka.
7. Krytyczne sytuacje audytu systemu zarządzania bezpieczeństwem informacji.
8. Podstawy audytowania – rodzaje audytów
9. Metody i techniki audytowania – planowanie (plan audytu, pytania audytowe / checklista) i przeprowadzanie audytu.
10. Sprawozdawczość z audytu, działania wynikające z audytu (korygujące, korekcyjne, doskonalące oraz zapobiegawcze), przygotowanie raportu z audytu bezpieczeństwa informacji.
11. Polityka bezpieczeństwa, organizacja bezpieczeństwa informacji.
12. Zarządzanie incydentami w bezpieczeństwie informacji.

Po zakończeniu szkolenia uczestnicy powinni m.in.:

1. zdobyć wiedzę praktyczną w oparciu o system zarządzania bezpieczeństwem informacji ISO/IEC 27001.
2. posiąść wiedzę jak przeprowadzić audyt efektywnie i zgodnie z wymaganiami procedury oraz wymaganiami ISO/IEC 27001.

Część 9: Szkolenie powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcje personelu, w szczególności sposób postępowania

specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia z zakresu socjotechnik, gdzie główny nacisk należy położyć na praktyczne umiejętności oraz testowanie reakcji personelu na różne scenariusze zagrożeń. Szkolenie stacjonarne ma odbyć się w 2 grupach, przy czym szkolenia tych grup nie mogą trwać jednocześnie, aby nie powodować utrudnień w ciągłości pracy danej Jednostki. W szkoleniu udział będzie brało około 40 pracowników. Szkolenie dla jednej grupy powinno trwać minimum 3 godziny zegarowe (łącznie z przerwami), powinno odbyć się w dni robocze, w godzinach pracy Urzędu Miejskiego w miejscu wskazanym przez Zamawiającego. Zamawiający oczekuje przeprowadzenia **dwóch rund testów**: przed rozpoczęciem i pod koniec szkolenia, w celu oceny stopnia przyswojenia wiedzy przez pracowników Urzędu. Wykonawca przedstawi Zamawiającemu pisemne podsumowanie wyników testów.

Testy muszą obejmować co najmniej:

1. Umiejętność wykorzystania wiedzy zdobytej podczas kursu w praktyce.
2. Zdolność do identyfikacji prób ataków socjotechnicznych i podejmowania odpowiednich kroków w celu ich zneutralizowania.
3. Postępowanie zgodnie z procedurami i rolami w SZBI.
4. Analizę wyników testów i wyciąganie wniosków z popełnionych błędów w celu poprawy przyszłych reakcji.

Wszystkie opracowane materiały szkoleniowe, certyfikaty, zaświadczenia muszą zawierać informację o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu „Cyberbezpieczny samorząd” oraz logotypy.

Zamawiający wymaga realizacji szkoleń według szczegółowego programu zawierającego informacje dotyczące tematyki i czasu szkolenia opracowanego przez Wykonawcę oraz dostarczonego Zamawiającemu na co najmniej 7 dni przed rozpoczęciem szkolenia. Zamawiający zastrzega sobie prawo wniesienia uwag do przedłożonego programu.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Struktura i cele Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie, jego aspekty praktyczne, a także rola i odpowiedzialność poszczególnych pracowników w jego funkcjonowaniu.
2. Polityki i procedury związane z bezpieczeństwem informacji obowiązujących w Urzędzie.
3. Sposoby poprawy procesów bezpieczeństwa informacji, takie jak ćwiczenia symulacyjne i audyty oraz rola pracowników Urzędu w tych procesach,
4. Rozpoznawanie zagrożeń, w tym rodzaje ataków, ransomware i malware, phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise oraz techniki stosowane w atakach socjotechnicznych, takie jak pretexting, baiting, vishing, atak

telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa.

5. Wpływ zagrożeń na działalność urzędu, w tym zrozumienie konsekwencji ataków cybernetycznych dla jednostki samorządu terytorialnego, ryzyka utraty danych, naruszenia bezpieczeństwa informacji oraz szkód reputacyjnych.
6. Ochrona danych i informacji, w tym podstawowe zasady ochrony danych osobowych i informacji wrażliwych, zgodnie z obowiązującymi przepisami (np. RODO) oraz środki ochrony, takie jak silne hasła, uwierzytelnianie wieloskładnikowe, klucze sprzętowe oraz bezpieczne zarządzanie hasłami.
7. Bezpieczeństwo systemów i urządzeń, w tym zasady bezpiecznego korzystania z urządzeń służbowych i systemów informatycznych, unikanie instalacji nieautoryzowanego oprogramowania i regularna aktualizacja systemów operacyjnych i aplikacji.
8. Reagowanie na incydenty bezpieczeństwa, w tym procedury zgłaszania incydentów bezpieczeństwa oraz sposoby ich dokumentowania, identyfikowanie potencjalnych incydentów i podejmowanie właściwych działań, współpraca z zespołem IT w celu rozwiązania problemów związanych z bezpieczeństwem oraz zrozumienie, kiedy i jak eskalować problemy do specjalistów.
9. Sposoby budowania kultury bezpieczeństwa, metody ciągłego doskonalenie umiejętności, dzielenie się wiedzą, audyty, promocja bezpieczeństwa informacji w codziennej pracy.
10. Szkolenia muszą być powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji specjalistów posiadających wyznaczone obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.