

Załącznik nr 6 do Regulaminu – Fiszka dla konkurencyjnego naboru nr FERS.01.13-IP.07-0001/25 stanowiąca Załącznik nr 5 do uchwały nr 112 Komitetu Monitorującego Program Fundusze Europejskie dla Rozwoju Społecznego 2021 – 2027 z dnia 28 listopada 2024 roku

Roczny Plan Działania na rok: 2025

Nazwa fiszki: Podniesienie kompetencji przedstawicieli i przedstawicielek zawodów związanych z ochroną zdrowia w zakresie zasad cyberbezpieczeństwa

Wersja fiszki: 1

Numer i data uchwały Komitetu Monitorującego: uchwała nr 112 z dnia 28 listopada 2024 r.

Informacje o instytucji opracowującej fiszkę

Instytucja: Ministerstwo Zdrowia

Dane kontaktowe osoby do kontaktów roboczych: Marta Fijołek - Naczelnik, Wydział Oceny i Monitorowania II, Departament Oceny Inwestycji, adres e-mail: m.fijolek@mz.gov.pl, nr telefonu: 882 359 166

Fiszka konkursu

Podstawowe informacje o konkursie

Numer i nazwa Priorytetu: FERS.01 Umiejętności

Numer i nazwa działania FERS: FERS.01.13 Umiejętności w sektorze zdrowia

Cel szczegółowy, w ramach którego projekty będą realizowane CP4.G Wspieranie uczenia się przez całe życie, w szczególności elastycznych możliwości podnoszenia i zmiany kwalifikacji dla wszystkich, z uwzględnieniem umiejętności w zakresie przedsiębiorczości i kompetencji cyfrowych, lepsze przewidywanie zmian i zapotrzebowania na nowe umiejętności na podstawie potrzeb rynku pracy, ułatwianie zmian ścieżki kariery zawodowej i wspieranie mobilności zawodowej (EFS+)

Typ projektu przewidziane do realizacji w ramach konkursu Rozwój i wsparcie kształcenia kadr organizacyjnych, administracyjnych i zarządzających systemu ochrony zdrowia

Planowany kwartał i rok ogłoszenia konkursu 1. kwartał 2025

Planowany miesiąc i rok rozpoczęcia naboru wniosków o dofinansowanie styczeń 2025

Tryb realizacji naboru

zamknięty

Czy w ramach konkursu będą wybierane projekty grantowe?

Nie

Rodzaj sposobu rozliczenia projektów

Inne

Planowana alokacja (PLN)

36 960 000,00

Wymagany wkład własny beneficjenta

Tak

Minimalny udział wkładu własnego w finansowaniu wydatków kwalifikowalnych projektu: 5%

Cross-financing

Nie

Główne grupy docelowe

- farmaceuci i pracownicy aptek,
- kadra podmiotów świadczących usługi zdrowotne (w tym m.in. pracownicy działów IT, kadry organizacyjne, administracyjne, zarządzające systemy ochrony zdrowia),
- pracownicy jednostek podległych, nadzorowanych przez Ministerstwo Zdrowia oraz pracownicy Ministerstwa Zdrowia.

Celem konkursu jest przeprowadzenie kształcenia dla 5200 osób stanowiących kadry systemu ochrony zdrowia w zakresie zasad cyberbezpieczeństwa poprzez:

- opracowanie programów, modułów i materiałów szkoleniowych z obszarów dotyczących cyberbezpieczeństwa, polityki bezpieczeństwa, przepisów RODO i ochrony danych w podmiotach leczniczych,
- organizację, przeprowadzenie i opracowanie analizy szkoleń dla grupy docelowej projektu.

Efektem konkursu będzie podniesienie kompetencji minimum 4420 osób stanowiących kadry systemu ochrony zdrowia w zakresie znajomości i stosowania zasad dot. cyberbezpieczeństwa.

Fiszka nie powiela zakresu udzielanego wsparcia w ramach interwencji Krajowego Planu Odbudowy i Zwiększania Odporności (KPO). Założenia niniejszej fiszki FERS są komplementarne względem interwencji KPO i tym

samym zwiększana będzie efektywność w osiągnięciu zamierzonych celów w programie FERS oraz planie KPO.

Zakładane efekty konkursu wyrażone wskaźnikami Wskaźniki rezultatu

1. Liczba osób, które podniosły swoje kompetencje dzięki udziałowi w szkoleniach oraz kształceniu podyplomowym prowadzonych w ramach programu

Wartość docelowa dla naboru: 4420

Wskaźniki produktu

1. Liczba osób, które wzięły udział w szkoleniach prowadzonych w ramach kształcenia podyplomowego

Wartość docelowa dla naboru: 5200

Szczegółowe kryteria wyboru projektów

Kryteria dostępu

1. **Podmiot uprawniony do złożenia wniosku o dofinansowanie oraz jego doświadczenie.**

Wnioskodawcą jest podmiot, który w ostatnich trzech latach kalendarzowych poprzedzających rok złożenia wniosku o dofinansowanie prowadził udokumentowaną działalność szkoleniową z zakresu cyberbezpieczeństwa w niżej wskazanych wszystkich 10 kluczowych obszarach, realizowaną na zlecenie innych podmiotów, o łącznej wartości co najmniej 1 mln zł, skierowaną do co najmniej 1000 uczestników (w sumie):

- 1) Bezpieczeństwo fizyczne (Physical Security);
- 2) Bezpieczeństwo sieci (Network Security);
- 3) Bezpieczeństwo informacji (Information Security);

- 4) Bezpieczeństwo aplikacji (Application Security);
- 5) Bezpieczeństwo operacyjne (Operational Security);
- 6) Bezpieczeństwo punktów końcowych (Endpoint Security);
- 7) Bezpieczeństwo chmury (Cloud Security);
- 8) Bezpieczeństwo mobilne (Mobile Security);
- 9) Bezpieczeństwo danych (Data Security);
- 10) Podstawy prawne oraz podstawowe informacje z zakresu przepisów RODO podmiotów leczniczych i ochrony wrażliwych danych medycznych.

Opis i uzasadnienie kryterium:

Kryterium będzie służyło wyborowi Wnioskodawcy, który posiada doświadczenie w prowadzeniu działalności szkoleniowej z zakresu cyberbezpieczeństwa.

W celu potwierdzenia spełnienia kryterium wymagane jest przedstawienie wykazu szkoleń z zakresu cyberbezpieczeństwa, które Wnioskodawca zrealizował w ciągu ostatnich trzech lat kalendarzowych poprzedzających rok złożenia wniosku, z przyporządkowaniem ich do 10 ww. obszarów kluczowych.

Dodatkowo, w celu potwierdzenia spełnienia kryterium Wnioskodawca przedstawi informacje potwierdzające doświadczenie, wydane przez podmioty, na zlecenie których zrealizował przedsięwzięcia szkoleniowe, z których wynika łączna wartość finansowa zrealizowanych przedsięwzięć i liczba uczestników.

Czy treść wniosku o dofinansowanie w części dotyczącej spełniania kryterium może być uzupełniana lub poprawiana w zakresie określonym w regulaminie wyboru projektów¹:
Nie

2. Potencjał kadrowy Wnioskodawcy.

Wnioskodawca musi zaangażować do realizacji projektu kadrę szkoleniową, która posiada co najmniej trzyletnie doświadczenie w zakresie prowadzenia szkoleń z cyberbezpieczeństwa lub co najmniej trzyletnie doświadczenie zawodowe na stanowisku związanym z cyberbezpieczeństwem.

W ramach kadry szkoleniowej posiadającej ww. doświadczenie (w zakresie prowadzenia szkoleń lub zawodowego na stanowisku związanym z cyberbezpieczeństwem) wymagane jest:

- a) co najmniej 20% kadry posiadającej kwalifikacje z zakresu cyberbezpieczeństwa, potwierdzone ważnymi certyfikatami (mającymi zastosowanie do 10 obszarów szkoleniowych określonych w kryterium nr 1) określonymi w rozporządzeniu Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa;
- b) co najmniej 50% kadry szkoleniowej posiadającej ukończone studia podyplomowe z zakresu cyberbezpieczeństwa lub wykształcenie 2 stopnia z zakresu cyberbezpieczeństwa;
- c) co najmniej 10% kadry szkoleniowej o kwalifikacjach wskazanych łącznie w pkt a) i b).

Opis i uzasadnienie kryterium: Powyższe służy wyborowi Wnioskodawcy, który posiada potencjał kadrowy z kompetencjami w

¹ Na podstawie art. 55 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027.

zakresie cyberbezpieczeństwa. W celu zapewnienia wysokiej jakości świadczonych usług szkoleniowych w systemie ochrony zdrowia, niezbędne jest odpowiednie przygotowanie merytoryczne kadry.

W celu spełnienia kryterium Wnioskodawca jest zobowiązany wykazać kadrę szkoleniową posiadającą ww. doświadczenie, przyporządkować ją zgodnie z posiadanymi kwalifikacjami do pkt. a), b) i c) i wykazać procentowy udział kadry o określonych kwalifikacjach.

Czy treść wniosku o dofinansowanie w części dotyczącej spełniania kryterium może być uzupełniana lub poprawiana w zakresie określonym w regulaminie wyboru projektów²?:
Nie

3. Grupa docelowa.

Projekt przewiduje, że działania szkoleniowe zostaną skierowane do wszystkich poniższych grup docelowych, które funkcjonują w ramach publicznego systemu ochrony zdrowia:

- farmaceutów i pracowników aptek,
- kadry podmiotów świadczących usługi zdrowotne (w tym m.in. kadra medyczna, pracownicy działów IT, kadry organizacyjne, administracyjne, zarządzające),
- pracowników jednostek podległych, nadzorowanych przez Ministerstwo Zdrowia oraz Ministerstwa Zdrowia.

Opis i uzasadnienie kryterium: Kryterium będzie służyło ukierunkowaniu wsparcia na te grupy docelowe, które kwalifikują się do objęcia wsparciem zgodnie z zapisami Programu Fundusze Europejskie dla Rozwoju Społecznego.

² Na podstawie art. 55 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027.

Czy treść wniosku o dofinansowanie w części dotyczącej spełniania kryterium może być uzupełniana lub poprawiana w zakresie określonym w regulaminie wyboru projektów³?:
Nie

4. Tematyka szkoleń.

Projekt przewiduje realizację szkoleń we wszystkich 10 kluczowych obszarach:

- 1) Bezpieczeństwo fizyczne (Physical Security);
- 2) Bezpieczeństwo sieci (Network Security);
- 3) Bezpieczeństwo informacji (Information Security);
- 4) Bezpieczeństwo aplikacji (Application Security);
- 5) Bezpieczeństwo operacyjne (Operational Security);
- 6) Bezpieczeństwo punktów końcowych (Endpoint Security);
- 7) Bezpieczeństwo chmury (Cloud Security);
- 8) Bezpieczeństwo mobilne (Mobile Security);
- 9) Bezpieczeństwo danych (Data Security);
- 10) Podstawy prawne oraz podstawowe informacje z zakresu przepisów RODO podmiotów leczniczych i ochrony wrażliwych danych medycznych;

w tym w odniesieniu do wdrażanych e-usług centralnych w obszarze e- zdrowia.

³ Na podstawie art. 55 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027

Opis i uzasadnienie kryterium: Wnioskodawca opracuje programy szkoleń dla wskazanych w kryterium nr 3 grup docelowych, dostosowane do ich potrzeb i wymagań, wynikających z rodzaju wykonywanej pracy, zakładające realizację wszystkich 10 obszarów kluczowych. Wnioskodawca stworzy materiały szkoleniowe (w formie elektronicznej, zgodnej z zasadami dostępności), które będą dostępne dla uczestników. Kryterium ma na celu zapewnienie, że wsparcie szkoleniowe będzie odnosić się do tematyki niezbędnej z punktu widzenia potrzeb sektora ochrony zdrowia. Każdy uczestnik będzie brał udział w szkoleniu we wszystkich 10 kluczowych obszarach. Wnioskodawca musi przeprowadzić ocenę wzrostu kompetencji po szkoleniu w celu określenia przyrostu wiedzy.

Czy treść wniosku o dofinansowanie w części dotyczącej spełniania kryterium może być uzupełniana lub poprawiana w zakresie określonym w regulaminie wyboru projektów⁴:
Nie

5. Zakres, czas i forma szkoleń dla pracowników podmiotów leczniczych i farmaceutów.

- a. Projekt przewiduje realizację szkoleń z podstaw cyberbezpieczeństwa dla pracowników podmiotów leczniczych (z wyłączeniem pracowników IT, kadry zarządzającej, pracowników MZ i pracowników jednostek podległych lub nadzorowanych przez MZ), farmaceutów, pracowników aptek, którzy na co dzień w bieżącej pracy korzystają z systemów teleinformatycznych, Internetu oraz urządzeń elektronicznych, które przetwarzają dane w podmiotach. Zakres merytoryczny szkoleń musi obejmować 10 obszarów kluczowych wskazanych w kryterium nr 4.
- b. Czas trwania i forma szkolenia: Wymagana jest organizacja 100 cykli szkoleniowych po 48 godzin (zegarowych) zajęć prowadzonych w modelu hybrydowym (25 % - wykłady, 60% - zajęcia interaktywne,

⁴ Na podstawie art. 55 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027.

warsztaty, pokazy, 15% - konsultacje), przewidzianych dla grup maksymalnie 20-osobowych. Materiały szkoleniowe muszą być dostępne dla uczestników w trybie ciągłym - w całym okresie realizacji projektu.

W ramach zadania wymagane jest przeszkolenie ok. 2000 osób.

Opis i uzasadnienie kryterium: Kryterium ma na celu zapewnienie, że wsparcie szkoleniowe będzie realizowane zgodnie z wymaganiami dotyczącymi czasu trwania, formy realizacji szkoleń oraz tematyki niezbędnej z punktu widzenia potrzeb sektora ochrony zdrowia.

Czy treść wniosku o dofinansowanie w części dotyczącej spełniania kryterium może być uzupełniana lub poprawiana w zakresie określonym w regulaminie wyboru projektów⁵:
Nie

6. Zakres, czas i forma szkoleń dla pracowników działów IT i pracowników odpowiadających za bezpieczeństwo informacji i cyberbezpieczeństwo w podmiotach leczniczych.

- a. Projekt przewiduje realizację szkoleń z cyberbezpieczeństwa dla pracowników działów IT i pracowników odpowiadających za bezpieczeństwo informacji i cyberbezpieczeństwo w podmiotach leczniczych. Zakres merytoryczny szkoleń musi obejmować 10 obszarów kluczowych wskazanych w kryterium nr 4, w tym m.in.:
- Podstawowe pojęcia związane z cyberbezpieczeństwem: Omówienie podstawowych zagrożeń, takich jak phishing, malware, ransomware i hakerstwo, a także zasad bezpiecznego korzystania z urządzeń elektronicznych,
 - Praktyczne zajęcia w środowisku symulacyjnym z identyfikacji podatności, symulacji ataków i metod przeciwdziałania zagrożeniom,

⁵ Na podstawie art. 55 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027.

- Bezpieczeństwo haseł i kont użytkowników: zapoznanie z zasadami tworzenia silnych haseł, unikalnych dla różnych kont użytkowników oraz sposobami przechowywania ich w bezpieczny sposób,
- Przedstawienie podstawowych narzędzi do zarządzania hasłami,
- Bezpieczeństwo sieci i urządzeń: omówienie zasad bezpieczeństwa w sieciach i na urządzeniach, takich jak stosowanie firewalli, szyfrowanie danych, aktualizacja systemów i oprogramowania antywirusowego,
- Bezpieczeństwo e-maili: zapoznanie z technikami rozpoznawania i unikania phishingowych wiadomości e-mail, w tym podejrzanych linków i załączników oraz sposobami reagowania na takie zagrożenia,
- Bezpieczeństwo przeglądania stron internetowych: omówienie zasad bezpiecznego korzystania z przeglądarki internetowej i unikania szkodliwych witryn internetowych,
- Bezpieczeństwo korzystania z mediów społecznościowych: omówienie zasad bezpiecznego korzystania z mediów społecznościowych, takich jak Facebook, Instagram, Twitter i LinkedIn, w tym ochrony prywatności i unikania nadużyć,
- Zabezpieczanie systemów i aplikacji: omówienie zasad zabezpieczania systemów i aplikacji przed atakami z zewnątrz oraz wewnętrznych zagrożeń, w tym uwierzytelnianie, kontrola dostępu i monitorowanie zdarzeń,
- Zgłaszanie i reagowanie na incydenty: przedstawienie sposobów zgłaszania podejrzanych działań oraz incydentów związanych z bezpieczeństwem informacji, w tym sposobów raportowania problemów, reagowania na incydenty i konsekwencji braku zgłaszania incydentów,
- Wybrane zagadnienia polityki bezpieczeństwa i przepisów RODO,

- Zapewnienie spełnienia wymagań w zakresie cyberbezpieczeństwa przy wdrażaniu e-usług centralnych (rozbudowa systemów gabinetowych/szpitalnych o integrację z usługami centralnymi): zdefiniowanie warunków integracji, przeprowadzenie testów akceptacyjnych/ bezpieczeństwa, kryteria odbioru testów akceptacyjnych/ bezpieczeństwa.
- b. Wymagana jest organizacja 80 cykli szkoleniowych po 64 godziny (zegarowe) zajęć, prowadzonych w modelu hybrydowym (25% - wykłady, 60% - zajęcia interaktywne, warsztaty, pokazy, 15% - konsultacje). Wnioskodawca musi przeprowadzić ocenę wzrostu kompetencji po szkoleniu w celu określenia przyrostu wiedzy. Po zakończonym cyklu w okresie max. 6 miesięcy uczestnicy muszą przyswoić wiedzę ze wskazanych modułów i przystąpić do oceny końcowej. Cykl szkoleniowy przewidziany jest dla grup max. 20 osobowych. W ramach zadania wymagane jest przeszkolenie ok. 1600 osób.

Opis i uzasadnienie kryterium: Kryterium ma na celu zapewnienie, że wsparcie szkoleniowe będzie realizowane zgodnie z wymaganiami dotyczącymi czasu trwania, formy realizacji szkoleń oraz tematyki niezbędnej z punktu widzenia potrzeb sektora ochrony zdrowia.

Czy treść wniosku o dofinansowanie w części dotyczącej spełniania kryterium może być uzupełniana lub poprawiana w zakresie określonym w regulaminie wyboru projektów⁶:
Nie

7. Zakres, czas i forma szkoleń dla kadry zarządzającej podmiotem leczniczym.

- a. Projekt przewiduje realizację szkoleń dla kadry zarządzającej podmiotem leczniczym, posiadającym umowę z Narodowym Funduszem Zdrowia na

⁶ Na podstawie art. 55 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027.

udzielanie świadczeń zdrowotnych. Zakres merytoryczny szkoleń musi obejmować 10 obszarów kluczowych wskazanych w kryterium nr 4, w tym m.in.:

- Wprowadzenie do cyberbezpieczeństwa: omówienie podstawowych pojęć i definicji związanych z cyberbezpieczeństwem, takich jak zagrożenia, ataki, ochrona i przepisy,
- Bezpieczeństwo haseł i kont użytkowników: zapoznanie z zasadami tworzenia silnych oraz unikalnych haseł dla różnych kont,
- Omówienie wymogów wynikających z przepisów dotyczących ochrony danych osobowych, w tym zasad wynikających z przepisów RODO,
- Bezpieczeństwo sieci i urządzeń: omówienie zasad ochrony sieci i urządzeń przed atakami, w tym stosowanie firewalli, szyfrowanie danych i wirtualnych sieci prywatnych (VPN),
- Zapoznanie z przepisami dotyczącymi ochrony danych w sieciach teleinformatycznych,
- Bezpieczeństwo e-maili: zapoznanie z technikami rozpoznawania i unikania phishingowych wiadomości e-mail, w tym podejrzanych linków i załączników. Omówienie zasad związanych z przetwarzaniem danych w poczcie elektronicznej,
- Politykę bezpieczeństwa: Omówienie zasad korzystania z systemów i zasobów informatycznych, odpowiedzialności za naruszenia bezpieczeństwa oraz procedur reagowania na incydenty,
- Zapoznanie z wymogami polityki informacyjnej podmiotu,
- Szkolenie pracowników: szkolenie pracowników w zakresie bezpieczeństwa IT, w tym zasad korzystania z systemów informatycznych, rozpoznawania zagrożeń i raportowania

podejrzanych działań. Omówienie przepisów dotyczących szkoleń w zakresie ochrony danych osobowych,

- Monitorowanie i raportowanie incydentów: metody monitorowania systemów informatycznych w celu wykrycia i zgłoszenia incydentów, w tym wykorzystanie systemów detekcji zagrożeń (IDS) i systemów zapobiegania zagrożeniom (IPS). Zapoznanie z przepisami dotyczącymi raportowania incydentów bezpieczeństwa informacji,
- Ochrona danych i zgodność z przepisami: zapewnienie ochrony prywatności i zgodność z przepisami dotyczącymi ochrony danych osobowych oraz monitorowanie i zarządzanie dostępem do poufnych informacji,
- Zapewnienie spełnienia wymagań w zakresie cyberbezpieczeństwa przy wdrażaniu e-usług centralnych (rozbudowa systemów gabinetowych/szpitalnych o integrację z usługami centralnymi): zdefiniowanie warunków integracji, przeprowadzenie testów akceptacyjnych/bezpieczeństwa, kryteria odbioru testów akceptacyjnych/bezpieczeństwa.

- b. Czas trwania i forma szkolenia: Wymagana jest organizacja 30 cykli szkoleniowych po 56 godzin (zegarowych) w modelu hybrydowym (25% - wykłady, 60% - zajęcia interaktywne (w tym stacjonarne), warsztaty, pokazy, 15% - konsultacje). Wnioskodawca musi przeprowadzić ocenę wzrostu kompetencji po szkoleniu w celu określenia przyrostu wiedzy. Po zakończonym cyklu w okresie max. 6 miesięcy uczestnicy muszą przyswoić wiedzę ze wskazanych modułów i przystąpić do oceny końcowej. Cykl szkoleniowy przewidziany jest dla grup max. 20 osobowych. W ramach zadania wymagane jest przeszkolenie ok. 600 osób.

Opis i uzasadnienie kryterium: Kryterium ma na celu zapewnienie, że wsparcie szkoleniowe będzie realizowane zgodnie z wymaganiami

dotyczącymi czasu trwania, formy realizacji szkoleń oraz tematyki niezbędnej z punktu widzenia potrzeb sektora ochrony zdrowia.

Czy treść wniosku o dofinansowanie w części dotyczącej spełniania kryterium może być uzupełniana lub poprawiana w zakresie określonym w regulaminie wyboru projektów⁷:

Nie

8. Zakres, czas i forma szkoleń dla pracowników jednostek podległych lub nadzorowanych przez MZ oraz pracowników MZ.

- a. Projekt przewiduje realizację szkoleń z podstaw cyberbezpieczeństwa dla pracowników jednostek podległych lub nadzorowanych przez MZ, oraz pracowników MZ. Zakres merytoryczny szkoleń musi obejmować 10 obszarów kluczowych wskazanych w kryterium nr 4, w tym m.in.:
- Podstawowe pojęcia związane z cyberbezpieczeństwem,
 - Omówienie podstawowych zagrożeń, takich jak phishing, malware, ransomware i hakerstwo, a także zasad bezpiecznego korzystania z urządzeń elektronicznych,
 - Bezpieczeństwo haseł i kont użytkowników: zapoznanie z zasadami tworzenia silnych haseł, unikalnych dla różnych kont użytkowników oraz sposobami przechowywania ich w bezpieczny sposób,
 - Przedstawienie podstawowych narzędzi do zarządzania hasłami. Bezpieczeństwo sieci i urządzeń: omówienie zasad bezpieczeństwa w sieciach i na urządzeniach, takich jak stosowanie firewalli, szyfrowanie danych, aktualizacja systemów i oprogramowania antywirusowego,

⁷ Na podstawie art. 55 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027.

- Bezpieczeństwo e-maili: zapoznanie z technikami rozpoznawania i unikania phishingowych wiadomości e-mail, w tym podejrzanych linków i załączników oraz sposobami reagowania na takie zagrożenia,
 - Bezpieczeństwo podczas przeglądania stron internetowych: omówienie zasad bezpiecznego korzystania z przeglądarki internetowej i unikania szkodliwych witryn internetowych,
 - Bezpieczeństwo podczas korzystania z mediów społecznościowych: omówienie zasad bezpiecznego korzystania z mediów społecznościowych, takich jak Facebook, Instagram, Twitter i LinkedIn, w tym ochrony prywatności i unikania nadużyć,
 - Zasady korzystania z urządzeń firmowych: omówienie zasad korzystania z urządzeń firmowych, takich jak komputery, laptopy, tablety i smartfony, w tym zasad odpowiedzialności za ich bezpieczeństwo i konsekwencje naruszeń,
 - Zgłaszanie incydentów: przedstawienie sposobów zgłaszania podejrzanych działań oraz incydentów związanych z bezpieczeństwem informacji, w tym sposobów raportowania problemów i konsekwencji braku zgłaszania incydentów,
 - Zapewnienie spełnienia wymagań w zakresie cyberbezpieczeństwa przy wdrażaniu e-usług centralnych (rozbudowa systemów gabinetowych/szpitalnych o integrację z usługami centralnymi): zdefiniowanie warunków integracji, przeprowadzenie testów akceptacyjnych/bezpieczeństwa, kryteria odbioru testów akceptacyjnych/bezpieczeństwa.
- b. Czas trwania i forma szkolenia: Wymagana jest organizacja 50 cykli szkoleniowych po 48 godzin (zegarowych) zajęć prowadzonych w modelu hybrydowym (25% - wykłady, 60% - zajęcia interaktywne, warsztaty, pokazy, 15% - konsultacje) przewidzianych dla grup

maksymalnie 20-osobowych). Materiały szkoleniowe muszą być dostępne dla uczestników w trybie ciągłym - w całym okresie realizacji projektu. W ramach zadania wymagane jest przeszkolenie ok. 1000 osób. Wnioskodawca musi przeprowadzić ocenę wzrostu kompetencji po szkoleniu w celu określenia przyrostu wiedzy.

Opis i uzasadnienie kryterium: Kryterium ma na celu zapewnienie, że wsparcie szkoleniowe będzie realizowane zgodnie z wymaganiami dotyczącymi czasu trwania, formy prowadzenia szkoleń oraz tematyki niezbędnej z punktu widzenia potrzeb sektora ochrony zdrowia.

Czy treść wniosku o dofinansowanie w części dotyczącej spełniania kryterium może być uzupełniana lub poprawiana w zakresie określonym w regulaminie wyboru projektów⁸:

Nie

9. Zakres, czas i forma szkoleń z RODO dla wszystkich grup docelowych.

- a. Projekt przewiduje realizację szkoleń z polityki bezpieczeństwa informacji na podstawie przepisów RODO dla całej grupy docelowej – poziom zaawansowany.

Wnioskodawca opracuje program szkolenia i stworzy materiały szkoleniowe (w formie elektronicznej, zgodnej z zasadami dostępności), które będą dostępne dla uczestników.

Program szkolenia obejmie m.in.: szczegółową analizę przepisów RODO, opracowywanie i wdrażanie polityk ochrony danych, ocenę ryzyka, zaawansowane zagadnienia ochrony systemów informacyjnych (m.in. systemy zarządzania tożsamością, techniki audytu), oraz praktyczne ćwiczenia i analizę przypadków, spełnienie wymagań RODO w

⁸ Na podstawie art. 55 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027.

kontekście przetwarzania danych pacjentów w ramach e-usług centralnych w obszarze e-zdrowia.

- b. Czas trwania i forma szkolenia: Wymagana jest organizacja jednodniowych szkoleń (przewidywana liczba godzin: 7 (zegarowych)). Szkolenia organizowane będą w formie on-line. Średnio w jednym szkoleniu udział weźmie 40 uczestników. Minimalna liczba uczestników szkolenia wyniesie 880 osób.
- c. Udział w szkoleniu możliwy będzie dla osób, które wcześniej wzięły udział w szkoleniach zdefiniowanych w kryterium nr 5,6,7,8 z zakresu cyberbezpieczeństwa i podstaw polityki RODO w podmiotach medycznych organizowanych w ramach projektu i uzyskały pozytywną ocenę wzrostu kompetencji weryfikującą poziom wiedzy po szkoleniu na min. 85%.

Opis i uzasadnienie kryterium: Kryterium ma na celu zapewnienie, że wsparcie szkoleniowe będzie realizowane zgodnie z wymaganiami dotyczącymi czasu trwania, formy prowadzenia szkoleń oraz tematyki niezbędnej z punktu widzenia potrzeb sektora ochrony zdrowia.

Czy treść wniosku o dofinansowanie w części dotyczącej spełniania kryterium może być uzupełniana lub poprawiana w zakresie określonym w regulaminie wyboru projektów?:

Nie

10. Zakres, czas i forma szkoleń z ochrony danych wrażliwych medycznych dla wszystkich grup docelowych.

- a. Projekt przewiduje realizację szkoleń z ochrony danych wrażliwych medycznych dla całej grupy docelowej – poziom zaawansowany.

Wnioskodawca opracuje program szkolenia. Wnioskodawca stworzy materiały szkoleniowe (w formie elektronicznej, zgodnej z zasadami dostępności), które będą dostępne dla uczestników.

Program szkoleń obejmie: zaawansowane Techniki Ochrony Danych Wrażliwych, zaawansowane metody zabezpieczania danych (pseudonimizacja, anonimizacja), technologie IT wykorzystywane w zabezpieczeniach danych (metody szyfrowania, systemy ochrony przed cyberatakami), audyty i ocena poziomu bezpieczeństwa, przetwarzanie danych pacjentów w ramach e-usług centralnych w obszarze e-zdrowia.

- b. Czas trwania i forma szkolenia: Wymagana jest organizacja jednodniowych szkoleń (przewidywana liczba godzin (zegarowych) : 7). Szkolenia organizowane będą w formie on-line. Średnio w jednym szkoleniu udział weźmie ok. 40 uczestników. Minimalna liczba uczestników szkolenia wyniesie 880 osób.
- c. Udział w szkoleniu możliwy będzie dla osób, które wcześniej wzięły udział w szkoleniach zdefiniowanych w kryterium nr 5,6,7,8 z zakresu cyberbezpieczeństwa i przepisów RODO w podmiotach, dla których zorganizowane zostało szkolenie w ramach projektu i uzyskały pozytywną ocenę wzrostu kompetencji weryfikującą poziom wiedzy po szkoleniu na min. 85%.
- d. Grupa docelowa: pracownicy podmiotów wykonujących działalność leczniczą, farmaceuci, pracownicy aptek, pracownicy jednostek podległych lub nadzorowanych przez MZ i pracownicy MZ.

Opis i uzasadnienie kryterium: Kryterium ma na celu zapewnienie, że wsparcie szkoleniowe będzie realizowane zgodnie z wymaganiami dotyczącymi czasu trwania, formy prowadzenia szkoleń oraz tematyki niezbędnej z punktu widzenia potrzeb sektora ochrony zdrowia.

Czy treść wniosku o dofinansowanie w części dotyczącej spełniania kryterium może być uzupełniana lub poprawiana w zakresie określonym w regulaminie wyboru projektów⁹: Nie

11. Analiza szkoleń

Projekt przewiduje opracowanie analizy z prowadzonych szkoleń, która obejmie minimum następujące aspekty:

- Ocena wiedzy i umiejętności uczestników: na podstawie przeprowadzonych ocen wzrostu kompetencji po szkoleniu w celu określenia przyrostu wiedzy.
- Opinie uczestników: na podstawie anonimowych ankiet pozwalających uczestnikom wyrazić swoje opinie na temat jakości szkoleń, przydatności materiałów oraz kompetencji prowadzących.
- Identyfikacja obszarów do poprawy: analiza wyników szkoleń pozwalających zidentyfikować elementy szkoleń, które wymagają poprawy lub zmiany, a także potencjalne tematy do przyszłych szkoleń.
- Zastosowanie wyników w praktyce: Wdrożenie rekomendacji wynikających z analizy w kolejnych edycjach szkoleń oraz innych programach rozwojowych, co przyczyni się do ciągłego doskonalenia oferty edukacyjnej.

Opis i uzasadnienie kryterium: Kryterium dotyczące opracowania analizy szkoleń pozwoli na ocenę efektywności realizowanych szkoleń. Wypracowana w projekcie analiza zostanie przekazana Ministrowi Zdrowia i będzie mogła być wykorzystana w kontekście podejmowanych przyszłych działań w zakresie zbieżnym z projektem.

⁹ Na podstawie art. 55 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027.

Czy treść wniosku o dofinansowanie w części dotyczącej spełniania kryterium może być uzupełniana lub poprawiana w zakresie określonym w regulaminie wyboru projektów¹⁰? : Nie

Kryteria premiujące

- 1) Wnioskodawca posiada udokumentowane minimum trzy pozytywne referencje od podmiotów, dla których zrealizował szkolenia z zakresu cyberbezpieczeństwa (niezależnie od szczegółowej tematyki szkolenia).**

Waga: 5 punktów – 3 referencje

6 punktów – 4 referencje

7 punktów – 5 referencji

8 punktów – 6 referencji

9 punktów – 7 referencji

10 punktów – 8 referencji

11 punktów – 9 referencji

12 punktów – 10 referencji

13 punktów – 11 referencji

14 punktów – 12 referencji

15 punktów – 13 referencji i więcej

Opis i uzasadnienie kryterium: Kryterium będzie służyło premiowaniu Wnioskodawcy, który posiada najwięcej pozytywnych referencji w zakresie realizacji szkoleń z cyberbezpieczeństwa. Do wniosku o dofinansowanie muszą zostać załączone referencje od co najmniej trzech podmiotów.

Referencje muszą zawierać informacje dotyczące formy prowadzonych

¹⁰ Na podstawie art. 55 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027.

szkoleń, tj. okres realizacji szkoleń, czas trwania szkoleń (liczba godzin, liczba dni), liczba uczestników, informacje dotyczące grupy docelowej odbiorców uczestniczących w szkoleniach.

2) Wnioskodawca przez co najmniej trzy ostatnie lata kalendarzowe poprzedzające rok złożenia wniosku prowadził udokumentowaną działalność szkoleniową z zakresu cyberbezpieczeństwa dla pracowników systemu ochrony zdrowia, we wszystkich 10 kluczowych obszarach:

- 1) Bezpieczeństwo fizyczne (Physical Security);
- 2) Bezpieczeństwo sieci (Network Security);
- 3) Bezpieczeństwo informacji (Information Security);
- 4) Bezpieczeństwo aplikacji (Application Security);
- 5) Bezpieczeństwo operacyjne (Operational Security);
- 6) Bezpieczeństwo punktów końcowych (Endpoint Security);
- 7) Bezpieczeństwo chmury (Cloud Security);
- 8) Bezpieczeństwo mobilne (Mobile Security);
- 9) Bezpieczeństwo danych (Data Security);
- 10) Podstawy prawne oraz podstawowe informacje z zakresu przepisów RODO podmiotów leczniczych i ochrony wrażliwych danych medycznych.

Waga: 5 punktów – 3 lata

6 punktów – 4 lata

7 punktów – 5 lat

8 punktów – 6 lat

9 punktów – 7 lat

10 punktów – 8 lat

11 punktów – 9 lat

12 punktów – 10 lat

13 punktów – 11 lat

14 punktów – 12 lat

15 punktów – 13 lat i więcej

Opis i uzasadnienie kryterium: Kryterium będzie służyło premiowaniu Wnioskodawcy, który posiada największe doświadczenie w prowadzeniu działalności szkoleniowej z zakresu cyberbezpieczeństwa dla pracowników systemu ochrony zdrowia. Wymagane jest przedstawienie wykazu szkoleń, które Wnioskodawca zrealizował w ciągu co najmniej trzech lat kalendarzowych poprzedzających rok złożenia wniosku.

- 3) Wnioskodawca zapewni, że do realizacji projektu zostanie zatrudniona lub oddelegowana osoba z niepełnosprawnością w wymiarze co najmniej ½ etatu, przez co najmniej połowę okresu realizacji projektu.**

Waga: 2 punkty

Opis i uzasadnienie kryterium: Kryterium ma na celu promowanie zaangażowania osób z niepełnosprawnością w projektach współfinansowanych ze środków Unii Europejskiej. Osoba z niepełnosprawnością to osoba w rozumieniu Wytycznych dotyczących realizacji zasad równościowych w ramach funduszy unijnych na lata 2021-2027. Kryterium weryfikowane na podstawie treści złożonego wniosku o dofinansowanie projektu. Koszt wynagrodzenia osoby z niepełnosprawnością może być kwalifikowany zarówno w ramach kosztów pośrednich, jak i bezpośrednich projektu.

Podpis osoby upoważnionej do podejmowania decyzji w zakresie Rocznego Planu Działania

Miejscowość, data: Warszawa, 11.12.2024 r.

Podpis osoby upoważnionej: Małgorzata Iwanicka-Michałowicz /zgodnie z podpisem
elektronicznym/

Data zatwierdzenia fiszki w ramach Rocznego Planu Działania:

(wypełnia Instytucja Zarządzająca FERS)