Zintegrowany Rejestr Kwalifikacji

Formularz dla kwalifikacji - podgląd

Typ wniosku

Wniosek o włączenie kwalifikacji do ZSK

Nazwa kwalifikacji*

Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych

Skrót nazwy

Paszport cyberbezpieczeństwa

Rodzaj kwalifikacji*

kwalifikacja cząstkowa

Proponowany poziom Polskiej Ramy Kwalifikacji*

3

Krótka charakterystyka kwalifikacji, obejmująca informacje o działaniach lub zadaniach, które potrafi wykonywać osoba posiadająca tę kwalifikacje oraz orientacyjny koszt uzyskania dokumentu potwierdzającego otrzymanie danej kwalifikacji*

Osoba posiadająca kwalifikację stosuje w swojej codziennej pracy zawodowej w instytucji finansowej, niezależnie od stanowiska czy obszaru działania, podstawowe zasady cyberbezpieczeństwa. Osoba posiadająca kwalifikację korzysta z urządzeń teleinformatycznych oraz aplikacji i systemów informatycznych w sposób bezpieczny i świadomy, minimalizujący ryzyko utraty poufnych danych w wyniku własnego działania lub działania osób trzecich. Rozpoznaje sytuacje podejrzane, związane z działaniami w cyberprzestrzeni i reaguje adekwatnie do tych sytuacji. Ponadto, edukuje klientów instytucji finansowych w zakresie bezpiecznego korzystania z urządzeń i systemów teleinformatycznych. Orientacyjny koszt uzyskania kwalifikacji – 400 zł.

Orientacyjny nakład pracy potrzebny do uzyskania kwalifikacji [godz.]*

35

Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji*

Kwalifikacja jest skierowana do każdego pracownika instytucji finansowej oraz infrastruktury finansowej, tzn. banku, ubezpieczyciela, agenta rozliczeniowego i in., mającego kontakt z technologiami cyfrowymi, które mogą stwarzać cyberzagrożenie w środowisku własnym pracy oraz dla klientów. Kwalifikacja odpowiada także na potrzeby pracowników firm i instytucji infrastruktury sektora finansowego, takich jak Krajowa Izba Rozliczeniowa, Biuro Informacji Kredytowej, firmy-outsourcerzy banków, pracownicy pośredników finansowych i agregatorów płatności i in. Kwalifikacja może być także użyteczna dla pracowników, mających kontakt z

reklamacjami i zgłoszeniami klientów, których działania mogą być narażone na cyberzagrożenia. Kwalifikacja będzie też wartościową propozycją dla studentów i absolwentów, którzy planują pracę w sektorze finansowym. Kwalifikacja będzie swego rodzaju „paszportem cyberbezpieczeństwa" pracownika instytucji finansowej.

Wymagane kwalifikacje poprzedzające

Opis

Kwalifikacja pełna z poziomem 4 PRK

Lista

W razie potrzeby warunki, jakie musi spełniać osoba przystępująca do walidacji*

Kwalifikacja pełna z poziomem 4 PRK

Zapotrzebowanie na kwalifikację*

Jak wskazują najnowsze badania (Raport „Nadużycia w sektorze finansowym", KPF, EY, 2017), cyberprzestępczość jest najszybciej rosnącym zagrożeniem dla branży finansowej. Liczba cyberataków, w tym ataków od wewnątrz instytucji, wzrosła w ciągu ostatnich 2 lat o 160%. Aktualnie trwają uzgodnienia projektu rozporządzenia Rady Ministrów w sprawie tzw. usług kluczowych. To akt wykonawczy do ustawy o krajowym systemie cyberbezpieczeństwa, która dotyczy implementacji dyrektywy Parlamentu Europejskiego i Rady (UE 2016/1148) z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej (The Directive on security of network and information systems, NIS Directive). Projektowana ustawa wpisuje się w cel 5. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, zakładający osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów informatycznych istotnych dla funkcjonowania państwa. Konsultowane Rozporządzenie obejmie 67 podmiotów: 20 największych banków, po 10 największych banków spółdzielczych, SKOK-ów, ubezpieczycieli, instytucji płatniczych oraz NBP, BGK, GPW, PWPW, KDPW i CCP. Bezsprzecznie istotnym elementem przygotowań do skutecznego działania w krajowej sieci bezpieczeństwa, zgodnie z ww. regulacjami, będzie potwierdzenie transparentnymi certyfikatami wiedzy i umiejętności pracowników, którzy są ważnym ogniwem tej sieci. W tym kontekście warto przytoczyć rekomendację Europejskiego Kongresu Finansowego 2017 w obszarze cyberbezpieczeństwa sektora finansowego, która postuluje „zdefiniowanie i określenie potrzeb sektora finansowego w zakresie profilu kompetencyjnego z obszaru cyberbezpieczeństwa, wypracowanie oraz wdrożenie odpowiedniego programu edukacyjnego przy współpracy z organami oświaty i administracji publicznej" (http://www.efcongress.com/sites/default/files/cyberbezpieczestwo_sektora_finansowego.pdf). Wspomniany program edukacyjny powinien kończyć się potwierdzeniem kwalifikacji. Według wyników najnowszego Sektorowego Badania Kompetencji Sektora Finansowego wśród stanowisk i kompetencji, na które w najbliższym czasie będzie rosło zapotrzebowanie w sektorze, znajduje się obszar cyberbezpieczeństwa (Raport SBKL 2018, SRK SF, dostępny na stronie internetowej Rady, www.rada.wib.org.pl). Jak podaje GUS (Zatrudnienie i wynagrodzenia w gospodarce narodowej w I kwartale 2018 r., GUS 2018, http://stat.gov.pl/obszary-tematyczne/rynek-pracy/pracujacy-zatrudnieni-wynagrodzenia-koszty-pracy/zatrudnienie-i-wynagrodzenia-w-gospodarce-narodowej-w-pierwszym-kwartale-2018-r-,1,30.html), wielkość zatrudnienia w działalności finansowej i ubezpieczeniowej wynosiła na

koniec marca 2018 r. 275,5 tysiąca. Ta wielkość wyznacza prognozę zapotrzebowania na proponowaną kwalifikację, a na pewno na posiadanie efektów uczenia się zawartych w przedkładanej kwalifikacji. W świetle powyższych procesów, trendów i prognoz, odczuwanej potrzeby zatrudniania pracowników posiadających aktualne umiejętności z zakresu stosowania zasad cyberbezpieczeństwa należy uznać, że efekty uczenia się zawarte w proponowanej kwalifikacji odpowiadają wprost na kluczowe potrzeby sektora finansowego, jego podmiotów i pracowników. Ich znaczenie będzie rosło w kolejnych latach, stając się ważnym elementem wzmacniania bezpieczeństwa systemu finansowego w Polsce. Źródła: ● Raport Nadużycia w sektorze finansowym z dn.24.10.2017, Konferencja Przedsiębiorstw Finansowych i EY. Raport dostępny: http://www.ey.media.pl/pr/373780/cyberprzestepczosc-najszybciej-rosnacym-zagrozeniem-wedlug-branzy-fina ● https://legislacja.rcl.gov.pl/projekt/12312201/katalog/12512907#12512907 ● https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive ● http://www.efcongress.com/sites/default/files/cyberbezpieczestwo_sektora_finansowego.pdf ● Raport Sektorowego Badania Kompetencji Sektora Finansowego (Sektorowa Rada ds. Kompetencji Sektora Finansowego) http://stat.gov.pl/obszary-tematyczne/rynek-pracy/pracujacy-zatrudnieni-wynagrodzenia-koszty-pracy/zatrudnienie-i-wynagrodzenia-w-gospodarce-narodowej-w-pierwszym-kwartale-2018-r-,1,30.html)

Odniesienie do kwalifikacji o zbliżonym charakterze oraz wskazanie kwalifikacji ujętych w ZRK zawierających wspólne zestawy efektów uczenia się*

Brak

Typowe możliwości wykorzystania kwalifikacji*

Osoba posiadająca kwalifikację "Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych", posiadając równocześnie wykształcenie kierunkowe związane z obszarem bankowości i finansów, może pracować w banku, bądź innej instytucji finansowej, a także instytucjach i firmach infrastruktury sektora finansowego, takich jak Krajowa Izba Rozliczeniowa, Biuro Informacji Kredytowej, firmy-outsourcerzy banków. Może też aplikować na stanowiska związane z bezpośrednią obsługą klienta, przyjmowaniem zgłoszeń klientów, a także wszędzie tam, gdzie jednym z zadań jest edukowanie klientów w zakresie podstaw cyberbezpieczeństwa: uświadamianie o zagrożeniach wynikających z funkcjonowania w cyberprzestrzeni oraz propagowanie zasady bezpiecznego korzystania z urządzeń i systemów teleinformatycznych.

Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację*

1. Etap weryfikacji 1.1. Metody 1. 1.1. Test teoretyczny (do zestawów 1-4) 1.1.2. Obserwacja w warunkach symulowanych (zadania praktyczne w formie mini-symulacji) - do wskazanych efektów uczenia się z zestawu 1-2: a. zestaw 1: Posługuje się hasłami do systemów informatycznych zgodnie z zasadami bezpieczeństwa; Używa komputera zachowując zasady bezpieczeństwa; Korzysta z poczty elektronicznej z zachowaniem zasad bezpieczeństwa b. zestaw 2: Wyjaśnia, jak korzystać z kart płatniczych zgodnie z zasadami bezpieczeństwa 1.1.3. Analiza dowodów i deklaracji (do efektu uczenia się „Stosuje Politykę Bezpieczeństwa firmy” w zestawie 4) a. W przypadku osoby, która jest zatrudniona, dla zaliczenia tego efektu uczenia się wymagane jest pisemne potwierdzenie przez pracodawcę, że uczestnik stosuje Politykę Bezpieczeństwa obowiązującą w jego firmie. b. Pozostali uczestnicy oraz osoby, które nie przedstawią ww. potwierdzenia, zaliczają ten efekt uczenia się poprzez dodatkowe pytania w ramach testu teoretycznego. 1.1.4. Analiza dowodów i deklaracji - po upływie 3 lat od daty

otrzymania certyfikatu, potwierdzenie przez pracodawcę, że osoba posiadająca kwalifikację, posiada zaktualizowane efekty uczenia się. Potwierdzenie jest wykorzystywane w celu podjęcia decyzji o przedłużeniu ważności certyfikatu. 1.2. Zasoby kadrowe Instytucja certyfikująca powołuje zespół walidacyjny, który projektuje i odpowiada za proces walidacji dla kwalifikacji „Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych". Członkowie zespołu walidacyjnego mogą pełnić funkcję doradcy walidacyjnego lub asesorów. Rola doradcy walidacyjnego polega na wspieraniu osób przystępujących do walidacji na wszystkich etapach tego procesu, w szczególności na etapie identyfikowania i dokumentowania. Zespół walidacyjny wyznacza komisję walidacyjną asesorów liczącą minimum 2 osoby, która odpowiada za weryfikację efektów uczenia się osób przystępujących do walidacji. Wszyscy członkowie zespołu walidacyjnego muszą posiadać kwalifikację pełną z poziomem 7 PRK. W zespole walidacyjnym musi się znaleźć przynajmniej dwóch praktyków rynkowych, z minimum 3-letnim doświadczeniem w obszarze bezpieczeństwa informacji i systemów informatycznych oraz minimum jedna osoba z przynajmniej 3-letnim doświadczeniem w projektowaniu rozwiązań walidacyjnych oraz w zakresie egzaminowania kadr bankowo-finansowych. 1.3. Sposób organizacji walidacji oraz warunki organizacyjne i materialne Na tym etapie walidacji wymagane jest: a. sprawdzenie tożsamości osób przystępujących do walidacji zgodnie z zarejestrowanym zgłoszeniem b. zapewnienie warunków lokalowych odpowiednich dla przeprowadzenia egzaminu w sposób gwarantujący zdającym samodzielność w udzielaniu odpowiedzi c. zapewnienie dostępu do stanowiska komputerowego dla każdej osoby przystępującej do walidacji, składającego się z komputera lub laptopa, z zainstalowanym następującym oprogramowaniem: ● system operacyjny Windows, ● dowolny program antywirusowy, ● dowolny program pocztowy, ze skonfigurowanym kontem umożliwiającym wysyłanie i odbieranie poczty elektronicznej, ● dowolna przeglądarka internetowa, ● oprogramowanie umożliwiające szyfrowanie danych: program kompresujący dane z hasłem lub program obsługujący format gpg. d. zapewnienie odpowiedniego nadzoru nad sprawnymi i transparentnym przebiegiem egzaminu - minimum 1 osoba nadzorująca na 25 osób przystępujących do egzaminu 2. Etapy identyfikowania i dokumentowania 2.1. Metody 2.1.1. Analiza dowodów i deklaracji a. Sprawdzenie prawidłowości i kompletności dokumentu potwierdzającego, że uczestnik stosuje Politykę Bezpieczeństwa obowiązującą w jego firmie b. Sprawdzenie prawidłowości i kompletności dokumentu potwierdzającego, że osoba posiadająca kwalifikację, posiada zaktualizowane efekty uczenia się - w przypadku osób posiadających certyfikat, które są zainteresowane przedłużeniem jego ważności. 2.2. Zasoby kadrowe Sprawdzenia dowodów dokonuje komisja walidacyjna (opis jak w pkt. 1.2) 2.3. Sposób organizacji walidacji Zapewnienie osobie przystępującej do walidacji możliwości kontaktu z doradcą walidacyjnym (telefonicznie, mailowo, bezpośrednio).

Propozycja odniesienia do poziomu sektorowych ram kwalifikacji (o ile dotyczy)

Nie dotyczy

Syntetyczna charakterystyka efektów uczenia się*

Osoba posiadająca kwalifikację „Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych" jest przygotowana do realizacji swoich obowiązków w instytucji finansowej zgodnie z zasadami cyberbezpieczeństwa. Bezpiecznie funkcjonuje w środowisku teleinformatycznym i korzysta w sposób bezpieczny z narzędzi i technologii funkcjonujących w bankach i instytucjach finansowych. Identyfikuje zagrożenia, przeciwdziała ryzyku cyberzagrożenia, sygnalizuje sytuacje podejrzane i raportuje naruszenia. Ponadto, może też edukować klientów w zakresie podstaw cyberbezpieczeństwa: uświadamiać o zagrożeniach wynikających z funkcjonowania w cyberprzestrzeni oraz propagować zasady bezpiecznego korzystania z urządzeń i systemów teleinformatycznych. Efekty uczenia się zawarte w kwalifikacji

potwierdzają: ● podstawy wiedzy z zakresu bezpieczeństwa w cyberprzestrzeni, w tym w szczególny sposób w sektorze finansowym, ● umiejętność wykonywania prostych czynności w środowisku teleinformatycznym, zgodnie z instrukcjami, ● że identyfikuje elementarne uwarunkowania pracy z użyciem nowoczesnych technologii w instytucji finansowej.

Zestawy efektów uczenia się

Numer zestawu w kwalifikacji*

1

Nazwa zestawu*

Bezpieczne korzystanie z urządzeń i systemów teleinformatycznych przez pracowników instytucji finansowych

Poziom PRK*

3

Orientacyjny nakład pracy [godz.]*

17

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

A. Posługuje się hasłami do systemów informatycznych zgodnie z zasadami bezpieczeństwa

Kryteria weryfikacji*

● Tworzy bezpieczne hasło ● Wymienia zasady przechowywania haseł ● Opisuje zasady ochrony haseł przed nieuprawnionym dostępem przez inne osoby ● Wyjaśnia powody i częstotliwość okresowej zmiany haseł ● Definiuje metodę dwuskładnikowego uwierzytelniania ● Wymienia zasady posługiwania się urządzeniami kryptograficznymi typu token/karta kryptograficzna

---

Efekt uczenia się

B. Używa komputera zachowując zasady bezpieczeństwa

Kryteria weryfikacji*

● Wymienia zasady ochrony komputera przed dostępem osób niepowołanych ● Omawia powody aktualizacji systemu operacyjnego i aplikacji ● Sprawdza poprawność ustawień dotyczących aktualizacji systemu operacyjnego i aplikacji ● Wymienia powody oraz zasady wykorzystywania oprogramowania antywirusowego ● Sprawdza poprawność działania programu antywirusowego i ustawienia aktualizacji bazy sygnatur wirusów ● Podaje objawy infekcji komputera przez złośliwe oprogramowanie ● Objaśnia zasady bezpiecznego korzystania z publicznych i niezaufanych sieci komputerowych ● Przedstawia powody oraz zasady tworzenia i przechowywania kopii zapasowych ważnych plików ● Podaje zasady bezpiecznego użytkowania nośników danych i przenośnych urządzeń teleinformatycznych

Efekt uczenia się

C. Korzysta ze smartfona zgodnie z zasadami bezpieczeństwa

Kryteria weryfikacji*

● Objaśnia zasady instalowania i aktualizacji oprogramowania na smartfonie ● Opisuje objawy infekcji smartfona oraz cechy złośliwego oprogramowania ● Wymienia zasady ochrony smartfona i danych na nim przechowywanych

Efekt uczenia się

D. Korzysta z poczty elektronicznej z zachowaniem zasad bezpieczeństwa

Kryteria weryfikacji*

● Rozpoznaje cechy charakterystyczne spamu, malware i phishingu ● Podaje sposoby reagowania na wymienione zagrożenia ● Stosuje zasady adresowania e-maili, zapewniające poufność korespondencji ● Stosuje zabezpieczenia komunikacji elektronicznej wysyłanej na zewnątrz, zapewniające poufność i integralność informacji

Numer zestawu w kwalifikacji*

2

Nazwa zestawu*

Edukowanie klientów instytucji finansowych w zakresie bezpiecznego korzystania z bankowości internetowej, mobilnej i kart płatniczych

Poziom PRK*

3

Orientacyjny nakład pracy [godz.]*

6

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

A. Informuje, jak korzystać z bankowości internetowej i mobilnej zgodnie z zasadami bezpieczeństwa

Kryteria weryfikacji*

● Objaśnia zasady bezpiecznego logowania się do bankowych serwisów internetowych ● Wymienia zasady dokonywania płatności w internecie i autoryzacji transakcji

Efekt uczenia się

B. Wyjaśnia, jak korzystać z kart płatniczych zgodnie z zasadami bezpieczeństwa

Kryteria weryfikacji*

● Tworzy bezpieczny pin do karty płatniczej ● Omawia zasady bezpiecznego przechowywania kart płatniczych i pinów do kart ● Przedstawia zasady korzystania z kart płatniczych przy płatnościach w terminalu, bankomacie i internecie

---

Numer zestawu w kwalifikacji*

3

Nazwa zestawu*

Ochrona tożsamości swojej i klientów instytucji finansowej

Poziom PRK*

3

Orientacyjny nakład pracy [godz.]*

3

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

A. Chroni dane identyfikacyjne swoje i klientów przed ujawnieniem osobom niepowołanym

Kryteria weryfikacji*

● Definiuje, co to są dane identyfikacyjne składające się na tożsamość danej osoby ● Opisuje zasady ograniczania ryzyka ujawnienia danych identyfikacyjnych w życiu prywatnym i w internecie ● Wymienia zasady i warunki udostępniania danych identyfikacyjnych swoich lub klienta innym osobom ● Wymienia zasady postępowania z dokumentami papierowymi i elektronicznymi, zawierającymi jakiekolwiek dane identyfikacyjne

---

Efekt uczenia się

B. Korzysta z serwisów internetowych i społecznościowych w sposób minimalizujący utratę tożsamości

Kryteria weryfikacji*

● Wymienia zasady i warunki umieszczania informacji zawierających dane identyfikacyjne swoje lub klientów w ogólnodostępnych serwisach internetowych ● Opisuje sytuacje, w których może dojść do utraty tożsamości w serwisach internetowych i jak ujawnione dane mogą być wykorzystane przez osoby niepowołane

---

Efekt uczenia się

C. Zapewnia bezpieczeństwo dokumentów identyfikacyjnych

Kryteria weryfikacji*

● Wyjaśnia, jak bezpiecznie przechowywać dokumenty identyfikacyjne (np. dowód osobisty, prawo jazdy, paszport) ● Wymienia organy, do których należy zgłosić utratę dokumentu zawierającego dane identyfikacyjne ● Opisuje ryzyko związane ze skanowaniem, kopiowaniem i fotografowaniem dokumentów identyfikacyjnych ● Wymienia zasady postępowania z kopiami fizycznymi i elektronicznymi dokumentów identyfikacyjnych

---

Numer zestawu w kwalifikacji*

4

Nazwa zestawu*

Stosowanie uniwersalnych przepisów zapewniających bezpieczeństwo informacji, infrastruktury teleinformatycznej, pracowników oraz klientów w instytucji finansowej

Poziom PRK*

3

Orientacyjny nakład pracy [godz.]*

9

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

A. Stosuje politykę bezpieczeństwa

Kryteria weryfikacji*

● Uzasadnia potrzebę klasyfikacji informacji i stosowania adekwatnych do danej klasyfikacji zasad ochrony i postępowania ● Wymienia powody oraz zasady bezpiecznego niszczenia dokumentów papierowych i elektronicznych oraz nośników danych ● Wymienia zasady ochrony dostępu do informacji przed osobami niepowołanymi ● Opisuje przykładową procedurę zgłaszania incydentów bezpieczeństwa ● Omawia zasady dostępu do pomieszczeń ● Objaśnia zasady "czystego biurka" (Clean Desk Policy) w miejscu pracy ● Opisuje zasadę niezbędnej wiedzy/informacji (tzw. Chinese Wall) ● Charakteryzuje generalne zasady kontaktu z mediami/klientami

---

Efekt uczenia się

B. Reaguje w sytuacjach próby popełnienia oszustwa przez cyberprzestępców

Kryteria weryfikacji*

● Opisuje najbardziej popularne oszustwa wykorzystujące metody socjotechniczne, na które

narażone są instytucje finansowe ● Wymienia symptomy próby oszustwa lub manipulacji ● Wymienia sposoby zapobiegania przestępstwom socjotechnicznym i postępowania w przypadku stwierdzenia oszustwa

Informacje o instytucjach uprawnionych do nadawania kwalifikacji

Wnioskodawca*

Fundacja Warszawski Instytut Bankowości

Minister właściwy*

Ministerstwo Cyfryzacji

Okres ważności dokumentu potwierdzającego nadanie kwalifikacji i warunki przedłużenia jego ważności*

Okres ważności certyfikatu - 3 lata. Przedłużenie ważności kwalifikacji na podstawie potwierdzenia przez pracodawcę osoby posiadającej kwalifikację, że posiada zaktualizowane efekty uczenia się. Instytucja certyfikująca publikuje na swojej stronie wzór formularza potwierdzenia. Niespełnienie tego warunku oznacza utratę ważności certyfikatu.

Nazwa dokumentu potwierdzającego nadanie kwalifikacji*

Certyfikat

Uprawnienia związane z posiadaniem kwalifikacji*

Nie dotyczy

Kod dziedziny kształcenia*

481 - Informatyka

Kod PKD*

62.02 - Działalność związana z doradztwem w zakresie informatyki

Status

Dokumenty

#	Tytuł dokumentu
1	potwierdzenie_przelewu_cyber
2	Statut WIB
3	Wniosek_stosowanie_zasad_cyberbezpieczenstwa
4	Wniosek_stosowanie_zasad_cyberbezpieczenstwa_skorygowany

☐ Oświadczam, że dane zawarte we wniosku o włączenie kwalifikacji rynkowej do Zintegrowanego Systemu Kwalifikacji są zgodne z prawdą. Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia.*

Dane o podmiocie, który złożył wniosek

Fundacja Warszawski Instytut Bankowości
Siedziba i adres: Solec 38 lokal 104, 00-394 Warszawa

NIP: 5260038522
REGON: 010189403
Numer KRS: 0000110584
Reprezentacja: Prezes zarządu samodzielnie lub dwóch członków zarząd łącznie lub członek zarządu działający z prokurentem. Prezes zarządu: Krzysztof Kokot Członkowie zarządu: Mariola Szymańska-Koszczyc, Wiceprezes Zarządu Waldemar Zbytek, Wiceprezes Zarządu Prokurenci: Małgorzata Gromiec Tomasz Jankowski

Adres elektroniczny osoby wnoszącej wniosek: mgromiec@wib.org.pl