PCO ACE-CRL - Program certyfikacji osób zarządzających podmiotami Krajowego Systemu Cyberbezpieczeństwa

[NASK-PIB DOKUMENT NR: PCO ACE-CRL/1.0]

NASK-PIB
ul. Kolska 12
01–045 Warszawa

standard@nask.pl
+48 22 380 82 00 / 01

NIP: 521 04 17 157
Regon: 010464542
KRS: 0000012938

www.certyfikacja.nask.pl

Spis treści

1. Cel i zakres stosowania

1 Dokument określa zasady certyfikacji osób zarządzających podmiotami Krajowego Systemu Cyberbezpieczeństwa[1] (KSC) poprzez ich niezależną ocenę zgodnie z kryteriami określonymi w niniejszym dokumencie oraz nadzoru nad certyfikacją prowadzoną przez Jednostkę Certyfikującą Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK-PIB).

2 Niniejszy program certyfikacji spełnia wymagania normy „PN-EN ISO/IEC 17024 Ocena zgodności. Ogólne wymagania dotyczące jednostek certyfikujących osoby".

3 Certyfikacja w zakresie niniejszego programu jest dobrowolna. Usługi certyfikacyjne NASK-PIB są otwarte dla wszystkich osób w sposób niedyskryminujący kogokolwiek.

4 NASK-PIB gwarantuje, że działania dotyczące certyfikacji realizowane są w sposób bezstronny i posiada zasoby adekwatne do przeprowadzenia procesu certyfikacji.

5 Właścicielem programu certyfikacji jest NASK-PIB.

6 Zakres programu i ogólne zasady certyfikacji są udostępniane poprzez stronę internetową www.certyfikacja.nask.pl Szczegółowe informacje dotyczące zasad i procedur certyfikacji można uzyskać w Jednostce Certyfikującej NASK-PIB: e-mail: standard@nask.pl.

7 Certyfikat jest poświadczeniem przez Jednostkę Certyfikującą NASK-PIB, że osoba, która go uzyskała spełnia wymagania określone w dokumentach normatywnych wskazanych w niniejszym programie.

2. Dokumenty powiązane

Dyrektywa Parlamentu Europejskiego I Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (NIS 2).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r poz. 913, 1703).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[1] Art. 4. Ustawy z dnia 5 lipca 2018 r, o Krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913, 1703).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565).

Rozporządzenie 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. z 2024 poz. 773).

Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (CSA).

Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. (Dz.U. z 2023 r. poz. 122).

Ustawa Prawo bankowe z dnia 29 sierpnia 1997 (Dz.U. z 2021 r. poz. 2439).

Ustawa Prawo telekomunikacyjne z dnia 16 lipca 2004 r. (Dz.U. z 2022 r. poz. 1648).

Ustawa Prawo energetyczne z dnia 10 kwietnia 1997 r. (Dz.U. z 2022 r. poz. 1385).

Ustawa Prawo pocztowe z dnia 23 listopada 2012 r. (Dz.U. z 2023 r. poz. 1640).

Ustawa o systemie ubezpieczeń społecznych z dnia 13 października 1998 r. (Dz.U. z 2023 r. poz. 1230).

Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U. z 2023 r. poz. 1703).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 1997 nr 88 poz. 553).

Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz.U. 1974 nr 24 poz. 141).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010 nr 182 poz. 1228).

PN EN ISO/IEC 27001 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania.

PN-EN ISO/IEC 22301 Bezpieczeństwo i odporność -- Systemy zarządzania ciągłością działania – Wymagania.

PN-EN ISO/IEC 19011 Wytyczne dotyczące auditowania systemów zarządzania.

PN-EN ISO/IEC 31000 Zarządzanie ryzykiem.

PN-EN ISO/IEC 17024 Ocena zgodności – Ogólne wymagania dotyczące jednostek certyfikujących osoby.

3. Definicje

8 Dla potrzeb niniejszego dokumentu, dokumentów powiązanych i wniosku o certyfikację stosuje się następujące definicje:

9 **Attested Cybersecurity Expert (ACE)** – nazwa rodziny programów certyfikacji osób w obszarze cyberbezpieczeństwa prowadzonych przez Jednostkę Certyfikującą NASK-PIB.

10 **Bezstronność** – zachowanie obiektywności.

11 **Certyfikat** – wydany przez Jednostkę Certyfikującą NASK-PIB dokument poświadczający, że przeprowadzona w wyniku umowy ocena kompetencji danej osoby została zakończona z wynikiem pozytywnym.

12 **Cofnięcie** – unieważnienie oświadczenia o zgodności.

13 **Cyber Resilience Leadership (CRL)** – nazwa kwalifikacji osoby, która pozytywnie przeszła proces oceny, zdała egzamin i uzyskała certyfikat kompetencji w zakresie niniejszego programu certyfikacji.

14 **Egzamin kwalifikacyjny** – egzamin przeprowadzany przez egzaminatora/komisję egzaminacyjną, w trakcie którego ocenia się wiedzę teoretyczną kandydata.

15 **Egzaminator** – osoba wyznaczona przez Kierownika Jednostki Certyfikującej NASK-PIB do przeprowadzania egzaminu zgodnie z programem certyfikacji.

16 **Jednostka certyfikująca** – oznacza Jednostkę Certyfikującą NASK-PIB.

17 **Kandydat** – wnioskujący, który spełnił wyspecyfikowane wstępne wymagania i został dopuszczony do procesu certyfikacji.

18 **Kierownik jednostki certyfikującej** – Kierownik Ośrodka Standaryzacji i Certyfikacji NASK-PIB, Dyrektor ds. certyfikacji NASK-PIB.

19 **Kompetencje** – zdolność stosowania wiedzy i umiejętności w celu osiągnięcia zamierzonych wyników.

20 **Nadzór** – systematyczne powtarzanie działań związanych z oceną zgodności jako podstawa do utrzymania ważności oświadczenia o zgodności.

21 **Niezgodność** – niespełnienie wymagania.

22 **Ocena** – niezależny, udokumentowany proces uzyskiwania dowodów, w celu określenia stopnia spełnienia wymagań, stanowiących kryteria certyfikacji.

23 **Odwołanie** – wystąpienie wnioskującego, kandydata lub osoby certyfikowanej o ponowne rozpatrzenie decyzji podjętej przez jednostkę certyfikującą dotyczącą jego oczekiwanego statusu certyfikacji.

24 **Osoba certyfikowana** – kandydat, który zdał egzaminu i zastała podjęta pozytywna decyzja o udzieleniu mu certyfikacji.

25 **Praktyka zawodowa** – doświadczenie w wykonywaniu czynności w zakresie określonym w programie.

26 **Ponowna certyfikacja** (recertyfikacja) – przedłużenie ważności wydanego certyfikatu na kolejny okres ważności, zgodnie z wymaganiami określonymi w niniejszym programie certyfikacji.

27 **Program certyfikacji** – dokument określający warunki i przebieg procesu certyfikacji w celu potwierdzenia kompetencji i innych wymagań dotyczących specyficznych kategorii zawodowych lub umiejętności osób.

28 **Proces certyfikacji** – działania związane z certyfikacją, łącznie z wnioskowaniem, oceną, decyzją w sprawie certyfikacji, ponownej certyfikacji i wykorzystywaniem certyfikatów oraz logo/znaków, za pomocą których jednostka certyfikująca ustala, że osoba spełnia wymagania certyfikacyjne.

29 **Rada Programu** – osoby powołane przez Kierownika Jednostki Certyfikującej NASK-PIB do opiniowania treści niniejszego programu oraz zatwierdzania pytań egzaminacyjnych.

30 **Skarga** – wyrażenie niezadowolenia innego niż odwołanie, przez jakąkolwiek osobę lub organizację, w stosunku do jednostki certyfikującej dotyczące działań tej jednostki lub osoby certyfikowanej, wymagające odpowiedzi.

31 **Umowa** – umowa o świadczenie usług certyfikacyjnych zawarta między NASK-PIB a wnioskującym, która obejmuje wykonanie przez NASK-PIB na zlecenie wnioskującego usług certyfikacyjnych.

32 **Wniosek o certyfikację** – standardowy formularz wypełniany przez wnioskującego, określający zakres usług certyfikacyjnych, jakie ma wykonać jednostka certyfikująca, wraz ze wszelkimi innymi informacjami dotyczącymi wykonania usług certyfikacyjnych.

33 **Wnioskujący** – osoba, która złożyła wniosek o dopuszczenie do procesu certyfikacji.

34 **Wymagania certyfikacyjne** – zbiór wyspecyfikowanych wymagań, łącznie z wymaganiami programu, które mają być spełnione w celu ustanowienia lub utrzymania certyfikacji.

4. Wymagania certyfikacyjne

35 Wymagania certyfikacyjne zostały określone w niniejszym „Programie certyfikacji osób zarządzających podmiotami Krajowego Systemu Cyberbezpieczeństwa" oraz dokumencie „Specyfikacja kryteriów i metodyka oceny dla Programu certyfikacji PCO ACE-CRL".

5. Zakres certyfikacji

36 Program skierowany jest dla osób zaangażowanych w zarządzanie podmiotami KSC, w tym w szczególności: członków zarządów, dyrektorów zarządzających, członków rad nadzorczych, dyrektorów generalnych, członków organu zarządzającego w podmiotach administracji publicznej (np. kierownik jednostki samorządu terytorialnego).

37 Pełna nazwa kwalifikacji potwierdzonych certyfikatem brzmi: Attested Cybersecurity Expert – Cyber Resilience Leadership (akronim: NASK-ACE-CRL). Nazwa występuje wyłącznie w języku angielskim.

5.1. Opis zakresu zastosowania i zadań osoby posiadającej certyfikat NASK-ACE-CRL

5.1.1. Opis zakresu zastosowania certyfikatu

38 Zakłada się, że osoba posiadająca certyfikat NASK-ACE-CRL ma wiedzę i umiejętności oraz jest odpowiedzialna za:

a) budowanie odporności podmiotu Krajowego Systemu Cyberbezpieczeństwa;

b) zapewnienie zgodności z wymaganiami formalno-prawnymi;

c) motywowanie do wdrażania i nadzoruje stosowanie dobrych praktyk dotyczących zarządzania podmiotami KSC;

d) nadzór nad systemem ciągłości działania podmiotu KSC ze szczególnym uwzględnieniem systemów informacyjno-komunikacyjnych (teleinformatycznych);

e) nadzór nad system zarządzania bezpieczeństwem informacji;

f) nadzór nad system zarządzania bezpieczeństwem informacji;

g) nadzór nad zarządzaniem ryzykiem w obszarze cyberbezpieczeństwa;

h) organizowanie i nadzór nad komunikacją w sytuacjach kryzysowych.

39 Zakłada się, że przygotowanie, kwalifikacja oraz utrzymanie ważności certyfikatu pozwala na doskonalenie warsztatu pracy kierującego podmiotem krajowego systemu

cyberbezpieczeństwa, członka rady nadzorczej, członka zarządu lub członka organu zarządzającego w podmiotach administracji publicznej.

40 Zakłada się, że uzyskany certyfikat jest potwierdzeniem merytorycznego przygotowania do zarządzania cyberbezpieczeństwem w podmiotach objętych przepisami Ustawy o krajowym systemie cyberbezpieczeństwa oraz Dyrektywą NIS 2.

5.1.2. Opis zadań

41 Osoba posiadająca certyfikat NASK-ACE-CRL wykonuje następujące zadania:

a) zapewnia budowanie odporności podmiotu KSC na zagrożenia z zakresu cyberbezpieczeństwa;

b) zapewnia ciągłość działania systemów teleinformatycznych;

c) nadzoruje wdrażanie wymagań formalno-prawnych dotyczących podmiotu KSC (wynikających z przepisów krajowych i europejskich) oraz dobrych praktyk;

d) nadzoruje proces identyfikacji zagrożeń i ochrony przed atakami cybernetycznymi;

e) nadzoruje proces zarządzania bezpieczeństwem informacji;

f) nadzoruje proces zgłaszania incydentów cyberbezpieczeństwa;

g) wdraża procedury komunikacji kryzysowej;

h) wdraża działania prewencyjne zwiększające cyberbezpieczeństwo;

i) wdraża środki zarządzania ryzykiem w cyberbezpieczeństwie;

j) zatwierdza wyniki szacowania ryzyka w obszarze cyberbezpieczeństwa.

5.2. Wymagania dotyczące kompetencji

42 Osoba certyfikowana posiada wiedzę z zakresu formalno-prawnych regulacji krajowych i Unii Europejskiej z obszaru cyberbezpieczeństwa, w tym w szczególności:

a) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;

b) Rozporządzenie 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.

c) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

d) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2);

e) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;

f) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

g) PN-EN ISO/IEC 27001 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

h) PN-EN ISO 22301 Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania.

43 Dodatkowo wskazana jest znajomość w zakresie właściwym do przedmiotu zagadnienia następujących aktów prawnych:

a) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie);

b) Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.;

c) Ustawa z dnia 6 czerwca 1997 r. Kodeks karny;

d) Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej;

e) Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne;

f) Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;

g) Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy.

44 Osoba certyfikowana posiada umiejętności nadzoru i koordynacji zadań w obszarze cyberbezpieczeństwa, w tym identyfikacji i reakcji na zagrożenia podmiotów KSC. Wie, jak zorganizować i nadzorować proces zgłaszania incydentów, zapewnić proces ciągłości działania sieci i systemów informacyjno-komunikacyjnych oraz nadzorować proces zarządzania bezpieczeństwem informacji.

45 Ponadto osoba certyfikowana posiada wiedzę w zakresie tworzenia strategii komunikacji kryzysowej oraz potrafi rozpoznać i zweryfikować informacje dotyczące ryzyka w obszarze cyberbezpieczeństwa. Zna metody i techniki związane z szacowaniem ryzyka.

46 Osoba certyfikowana zna dobre praktyki w zakresie zapewnienia bezpieczeństwa teleinformatycznego, sposoby ich wdrażania oraz możliwości certyfikacji produktów, procesów, usług i kompetencji personelu w zakresie cyberbezpieczeństwa.

47 Weryfikacja posiadania kompetencji następuje poprzez spełnienie przez kandydata wymagań wstępnych i przystąpienie do egzaminu. Szczegóły opisano odpowiednio w sekcji 6.2 „Warunki ubiegania się o certyfikację" i 6.3 „Ocena" a w przypadku ponownej certyfikacji w sekcji 6.9 „Ponowna certyfikacja" niniejszego programu certyfikacji.

6. Zasady certyfikacji

6.1. Informacje wstępne

48 Proces certyfikacji obejmuje złożenie wniosku przez osobę ubiegającą się o certyfikację w Jednostce Certyfikującej NASK-PIB, przegląd wniosku, ocenę, wydanie decyzji o certyfikacji oraz nadzór nad wydanym certyfikatem.

49 Jednostka Certyfikująca NASK-PIB zapewnia równy, niedyskryminujący dostęp do certyfikacji kompetencji.

50 Wnioskujący wymagający specjalnych warunków podejścia do egzaminu, zgłaszają ten fakt we wniosku o certyfikację. Możliwości organizacyjne przeprowadzenia egzaminu w takim przypadku są określane na podstawie uzgodnień pomiędzy Jednostką Certyfikująca NASK-PIB a wnioskującym.

51 Jednostka Certyfikująca NASK-PIB zapewnia, że działa w ramach wymagań normy PN-EN ISO/IEC 17024 oraz wszelkie podejmowane decyzje, są wolne od wszelkich nacisków, które mogłyby zagrozić obiektywności procesu certyfikacji.

52 Ponadto Jednostka Certyfikująca NASK-PIB:

a) jest odpowiedzialna za wydawanie certyfikatów;

b) zapewnia, że pytania egzaminacyjne nie są stosowane do celów szkoleniowych.

53 Wnioskujący potwierdza prawdziwość i ważność wszystkich danych przedstawianych we wniosku o certyfikację oraz zobowiązuje się do:

a) powiadamiania Jednostki Certyfikującej NASK-PIB o braku spełniania wymogów programu certyfikacji i innych wymagań mogących mieć wpływ na certyfikację;

b) nieujawniania treści materiałów egzaminacyjnych osobom trzecim.

6.2. Warunki ubiegania się o certyfikację

6.2.1. Wymagania wstępne

54 Kandydat do certyfikacji powinien spełniać następujące warunki:

a) wykształcenie wyższe;

b) co najmniej 5-letni okres zatrudnienia na podstawie umowy o pracę, powołania, wyboru, mianowania, spółdzielczej umowy o pracę lub świadczenia usług na podstawie innej umowy lub wykonywania działalności gospodarczej na własny rachunek;

c) co najmniej 5-letnie doświadczenie na stanowiskach kierowniczych lub samodzielnych albo wynikające z prowadzenia działalności gospodarczej na własny rachunek albo ukończone studia podyplomowe na kierunku zarządzanie i co najmniej 3-letni staż pracy;

d) co najmniej 2-letnie doświadczenie na stanowisku kierowniczym w podmiocie KSC (członek zarządu, członek rady nadzorczej, dyrektor generalny, kierujący jednostką samorządu terytorialnego) lub spełnia wymagania dla audytorów określone w przepisach wydanych na podstawie Art. 15 ust. 8 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r poz. 913, 1703);

e) brak skazania prawomocnym wyrokiem sądu za przestępstwo umyślne;

f) ukończenie szkolenia obejmującego wskazane w Programie certyfikacji moduły i ich minimalny wymiar czasowy określony w Tabeli 1.

55 Jednostka Certyfikująca NASK-PIB zastrzega sobie prawo do weryfikacji spełnienia powyższych wymagań.

6.2.2. Szkolenia

56 Wnioskujący o certyfikację w Jednostce Certyfikującej NASK-PIB powinien przedstawić zaświadczenie o ukończeniu szkolenia, obejmujące zakresem tematyki wymagania określone przez Jednostkę Certyfikującą NASK-PIB.

57 Zaświadczenie takie może być zaakceptowane jako dowód, jeśli dostarcza informacji, że program kursu szkolenia spełniał wymagania programu certyfikacji.

58 Zagadnienia szczegółowe tematyki szkolenia wymagane w niniejszym Programie Certyfikacji przedstawiono w Tabeli 1 poniżej.

Lp.	Moduł	Czas
1.	Wymaganie prawne dotyczące podmiotu KSC	2h
2.	Cyberbezpieczeństwo - podstawy	1h
3.	Budowanie odporności podmiotu KSC	2h
4.	Ciągłość działania systemów teleinformatycznych	2h
5.	Zarządzanie bezpieczeństwem informacji	2h
6.	Komunikacja kryzysowa	2h
7.	Szacowanie ryzyka w obszarze cyberbezpieczeństwa	4h
	Razem	**15**

Tabela 1 – Zakres programu szkolenia

6.2.3. Wniosek i umowa o certyfikację

59 Wniosek o certyfikację stanowi zlecenie dla Jednostki Certyfikującej NASK-PIB przeprowadzenia procesu certyfikacji na warunkach określonych w niniejszym Programie i jest potwierdzeniem przez wnioskującego akceptacji określonych w nim warunków.

60 Poprzez złożenie wniosku o certyfikację wnioskujący wyraża zgodę na spełnienie wymagań certyfikacyjnych oraz dostarczenie informacji potrzebnych do oceny.

61 Zapoznanie się przez osobę wnioskującą z postanowieniami niniejszego dokumentu oraz ich zaakceptowanie, potwierdzone podpisem złożonym na wniosku o certyfikację, stanowi wyrażenie zgody na zawarcie umowy o certyfikację.

62 Umowa zostaje zawarta z dniem przyjęcia do realizacji przez Kierownika Jednostki Certyfikującej NASK PIB (lub osoby upoważnionej) wniosku przesłanego przez osobę wnioskującą o certyfikację. Wniosek o certyfikację jest integralną częścią umowy o certyfikację.

63 Wnioskujący składa wniosek o certyfikację wraz odpowiednimi załącznikami. Formularz wniosku jest dostępny na stronie internetowej https://certyfikacja.nask.pl

64 Wnioskujący załącza do wniosku:

a) Kopie dokumentów potwierdzających spełnienie wymagań wstępnych;

b) Kopię zaświadczenia dokumentującego ukończenie odpowiedniego szkolenia;

c) Dowód wpłaty za rozpatrzenie wniosku.

65 W przypadku niespełnienia powyższych warunków, Jednostka Certyfikująca NASK-PIB informuje pisemnie wnioskującego o braku możliwości przeprowadzenia procesu certyfikacji z podaniem przyczyny.

66 W przypadku podania niepełnych danych, wnioskujący jest informowany o konieczności dokonania niezbędnych uzupełnień.

67 Jednostka Certyfikująca NASK-PIB sprawdza prawidłowość wypełnienia wniosku i ocenia spełnienie warunków przystąpienia do certyfikacji przez wnioskującego.

68 W przypadku spełnienia warunków przystąpienia do certyfikacji, wnioskujący otrzymuje pisemne zawiadomienie o miejscu i dacie egzaminu, informację o warunkach egzaminu oraz wysokości opłaty i numerze konta bankowego, na które należy wnieść opłatę certyfikacyjną przed przystąpieniem do egzaminu.

69 Jednostka Certyfikująca NASK-PIB w szczególnych przypadkach (np. ponoszenia kosztów egzaminu przez pracodawcę wnioskującego) dopuszcza przystąpienie do egzaminu bez wcześniejszego wniesienia opłaty, przy czym po egzaminie wystawiana jest faktura do zapłaty.

6.3. Ocena

6.3.1. Przeprowadzanie i nadzorowanie egzaminu

70 Egzaminy odbywają się w ośrodkach egzaminacyjnym NASK-PIB lub innym ośrodku działającym pod nadzorem NASK-PIB.

71 Egzamin może być przeprowadzony za pomocą środków teleinformatycznych służących do połączeń audio i video zweryfikowanych i zatwierdzonych przez Jednostkę Certyfikującą NASK-PIB do wykorzystania podczas egzaminu.

72 Kandydat otrzymuje informację o wymaganiach dotyczących sprzętu IT i warunkach jakim ma odpowiadać pomieszczenie, w którym odbywa się egzamin zdalny, wraz z informacją o dacie egzaminu.

73 Egzaminy są oceniane przez egzaminatorów powołanych przez Kierownika Jednostki Certyfikującej NASK-PIB. Egzaminatorzy podpisują oświadczenie o poufności i bezstronności; w szczególności egzaminator nie może weryfikować wiedzy kandydata, którego szkolił w ciągu ostatnich dwóch lat, licząc od daty zakończenia działań szkoleniowych.

74 Zestawy pytań testowych wybierane są z puli zatwierdzonej przez Radę Programu.

6.3.2. Zasady egzaminu

75 Podczas egzaminu kandydat powinien posiadać ważny dokument (ze zdjęciem) potwierdzający tożsamość (np. dowód osobisty lub paszport).

76 Podczas egzaminu pisemnego kandydat samodzielnie odpowiada na pytania testowe lub rozwiązuje zadania praktyczne. Nie jest dozwolona komunikacja z innymi egzaminowanymi osobami.

77 Podczas egzaminu nie jest dozwolone korzystanie z materiałów zewnętrznych. Podczas trwania egzaminu nie dopuszcza się posiadania przy sobie i korzystania z pomocy, takich jak, np. smartfon, telefon komórkowy, materiały papierowe (w tym książki), słuchawki.

78 Egzaminator informuje kandydatów przystępujących do egzaminu o zasadach i przebiegu egzaminu oraz o czasie jaki jest określony przez Jednostkę Certyfikującą NASK-PIB na udzielenie odpowiedzi lub wykonanie zadań.

79 Przystępując do egzaminu kandydat zobowiązuje się do nieujawniania treści materiałów egzaminacyjnych.

80 Przez cały czas trwania egzaminu obecna jest osoba nadzorująca egzamin lub egzaminator.

81 Każdy kandydat, który nie przestrzega zasad przebiegu egzaminu, w tym w szczególności posługuje się wyposażeniem, materiałami lub dokumentami, które mogą sugerować, że oszukuje lub pomaga w oszukiwaniu, może zostać wykluczony z dalszego udziału w egzaminie.

82 Jednostka Certyfikująca NASK-PIB w przypadku wykluczenia z egzaminu zastrzega sobie prawo do ustalenia karencji w zakresie powtórnego podejścia do egzaminu danego kandydata. Okres karencji nie może przekroczyć 12 miesięcy.

6.3.3. Egzamin

83 Egzamin jest przeprowadzany w formie pisemnej i trwa 80 minut. Składa się z 30 pytań testowych jednokrotnego lub wielokrotnego wyboru i 7 pytań otwartych, na które odpowiedź jest udzielana w formie opisowej.

84 Można uzyskać maksymalnie 44 punkty tj. 1 punkt za prawidłową odpowiedź z części testowej oraz 2 punkty za każdą pełną prawidłową odpowiedź z części pytań opisowych (w przypadku częściowej odpowiedzi można uzyskać 1 punkt za pytanie otwarte).

85 Aby zdać egzamin, kandydat powinien uzyskać nie mniej niż 70% prawidłowych odpowiedzi (31 punktów).

86 Wynik egzaminu kwalifikacyjnego odnotowuje egzaminator w protokole sporządzanym z egzaminu.

87 O wynikach egzaminu kandydat zostaje poinformowany przez Jednostkę Certyfikującą NASK-PIB niezwłocznie po egzaminie.

6.3.4. Egzamin poprawkowy

88 W przypadku negatywnego wyniku egzaminu kandydat może przystąpić do egzaminu poprawkowego.

89 Jedno podejście do egzaminu poprawkowego jest bezpłatne. Kolejne podejście wymaga wniesienia opłaty egzaminacyjnej.

90 Egzamin poprawkowy może odbyć się nie wcześniej niż po 1 miesiącu od daty egzaminu zakończonego wynikiem negatywnym.

6.4. Decyzja w sprawie certyfikacji

91 W przypadku pozytywnego wyniku egzaminu, Kierownik Jednostki Certyfikującej NASK-PIB podejmuje decyzję o udzieleniu certyfikacji i wydaje certyfikat.

92 Jednostka Certyfikująca NASK-PIB zachowuje prawo własności każdego wydanego certyfikatu.

93 Maksymalny czas na wydanie decyzji w sprawie certyfikacji wynosi 10 dni roboczych od daty egzaminu.

94 Certyfikat przyznawany jest na okres 2 lat, z wyjątkiem wprowadzenia zmian w warunkach przyznawania certyfikatów, nieprzestrzegania warunków korzystania z certyfikatu lub wyraźnej rezygnacji z certyfikacji wyrażonej przez osobę certyfikowaną.

95 Certyfikat zawierać będzie co najmniej poniższe informacje:

a) nazwę i adres jednostki certyfikującej;

b) identyfikator certyfikatu;

c) datę udzielenia certyfikacji;

d) imię i nazwisko certyfikowanej osoby;

e) zakres certyfikacji;

f) nazwę i akronim programu certyfikacji;

g) okres lub datę ważności certyfikacji;

h) podpis osoby upoważnionej do wydania certyfikatu.

96 W przypadku negatywnej decyzji dotyczącej wydania certyfikatu, kandydat ubiegający się o certyfikację może złożyć odwołanie od ww. decyzji na zasadach określonych w sekcji „Skargi i odwołania".

Uwaga: W przypadku zniszczenia lub zaginięcia certyfikatu istnieje możliwość odpłatnego wydania duplikatu na pisemny wniosek osoby certyfikowanej. Na życzenie osoby certyfikowanej certyfikat jest wydawany w formie dokumentu elektronicznego.

6.5. Ważność wydawanych dokumentów

97 Certyfikat jest ważny 2 lata. Data wydania i data ważności podane są na certyfikacie.

98 Jednostka Certyfikująca NASK-PIB zastrzega sobie prawo unieważnienia certyfikatu w przypadku posiadania dowodów postępowania osób certyfikowanych niezgodnego z zasadami określonymi w programie certyfikacji, w szczególności w przypadku:

a) posługiwania się certyfikatem przez osobę certyfikowaną w sposób nieuprawniony;

b) uzasadnionych skarg na osobę certyfikowaną lub postępowania w sposób rażąco naruszający podstawowe zasady etyki opisane w programie.

99 Unieważnienie certyfikatu może nastąpić również na wniosek osoby certyfikowanej.

6.6. Zawieszenie ważności certyfikatu

100 Zawieszenie ważności certyfikatu może nastąpić w przypadku:

a) zgłoszenia czasowej rezygnacji z certyfikatu przez osobę certyfikowaną;

b) stwierdzenia w ramach nadzoru nad certyfikatem niespełnienia wymagań związanych z wykorzystywaniem certyfikatów.

101 Certyfikat może być przywrócony na wniosek osoby certyfikowanej.

6.7. Cofnięcie certyfikatu

102 Cofnięcie certyfikatu może nastąpić w przypadku:

a) niespełnienia w ustalonym terminie warunków postawionych w decyzji o zawieszeniu certyfikatu;

b) rezygnacji osoby certyfikowanej z certyfikatu.

103 W przypadku cofnięcia certyfikatu możliwe jest ubieganie się ponowną o certyfikację po upływie co najmniej 6 miesięcy od daty cofnięcia.

104 W przypadku otrzymania decyzji o cofnięciu lub bez oddzielnego powiadomienia w przypadku zakończeniu certyfikacji, osoba certyfikowana zobowiązana jest do zaprzestania powoływania się na udzieloną certyfikację.

6.8. Nadzór nad certyfikacją

105 W okresie ważności certyfikatu Jednostka Certyfikująca NASK-PIB sprawuje nadzór poprzez:

a) rozpatrywanie skarg dotyczących osoby certyfikowanej;

b) potwierdzenie spełniania wymagań certyfikacyjnych w zakresie przedłużania ważności certyfikatu.

106 Działania prowadzone w ramach nadzoru mogą spowodować zawieszenie, ograniczenie lub cofnięcie certyfikatu przez Jednostkę Certyfikującą NASK-PIB.

6.9. Ponowna certyfikacja

107 Możliwość przedłużenia na kolejne 2 lata ważności certyfikatu jest warunkowana spełnieniem przedstawionych poniżej wymogów kształcenia ustawicznego i praktyki zawodowej:

a) Odbycie szkolenia lub szkoleń o tematyce określonej w sekcji „Szkolenia" w wymiarze łącznym co najmniej 5 godzin rocznie lub 10 godzin w ciągu dwóch lat;

b) Praktyka zawodowa na stanowisku/stanowiskach związanym z wykonywaniem zadań w ramach podmiotu KSC określonych w sekcji „Opis zadań" w okresie co najmniej pół roku, liczonego dla pełnego etatu umowy o pracę.

108 Jednostka Certyfikująca NASK-PIB zastrzega sobie prawo do weryfikacji spełnienia wymagań dotyczących praktyki zawodowej w przypadku pracy na stanowiskach niewymienionych powyżej, a pokrewnych specjalności lub zatrudnienia na podstawie umowy cywilnoprawnej.

109 Warunkiem przedłużenia ważności certyfikatu jest:

a) złożenie przez osobę certyfikowaną co najmniej 1 miesiąc przed upływem ważności certyfikatu wniosku o przedłużenie certyfikacji wraz z dokumentacją potwierdzająca spełnienie warunków kształcenia ustawicznego lub praktyki zawodowej;

b) wniesienie opłaty certyfikacyjnej.

110 W przypadku niespełnienia warunków określonych powyżej, dotyczących dokumentacji odpowiednich szkoleń kandydat może uzyskać ponownie certyfikację w trybie pełnego procesu certyfikacji określonego w niniejszym programie.

6.10. Postępowanie w przypadku zawieszenia lub cofnięcia certyfikacji

111 W przypadku zawieszenia lub cofnięcia certyfikacji osoba certyfikowana oświadcza, że zaprzestanie stosowania wszelkich deklaracji zawierających jakiekolwiek powołanie się na Jednostkę Certyfikującą NASK-PIB i na certyfikację.

112 W przypadku cofnięcia certyfikacji osoba certyfikowana niezwłocznie zwróci Jednostce Certyfikującej NASK-PIB wydane certyfikaty.

113 Osoba certyfikowana oświadcza, że niezwłocznie poinformuje Jednostkę Certyfikującą NASK-PIB o sprawach, które mogłyby mieć wpływ na jego zdolność do dalszego spełniania wymagań certyfikacyjnych.

6.11. Zmiany mające wpływ na certyfikację

114 W przypadku wystąpienia zmiany wymagań stanowiących podstawę certyfikacji, Jednostka Certyfikująca NASK-PIB przekazuje osobom certyfikowanym informację o zakresie zmian oraz o terminie ich wdrożenia w celu utrzymania udzielonej certyfikacji. Zmiany mające wpływ na certyfikację mogą wynikać z informacji uzyskanych przez Jednostkę Certyfikującą NASK-PIB już po rozpoczęciu certyfikacji (np. zmiany powszechnie obowiązującego prawa, warunków akredytacji itd.).

115 Informacje o zmianach będą przesyłane osobom certyfikowanym drogą elektroniczną.

116 Jeśli będzie to konieczne, działania dotyczące wdrażania zmian mogą obejmować w szczególności ponowną ocenę, w tym egzamin i decyzję o certyfikacji oraz wydanie dokumentów certyfikacyjnych zmieniających zakres certyfikacji.

117 Jednostka Certyfikująca NASK-PIB przedstawia osobom certyfikowanym sposób weryfikacji wdrożenia wymagań. W przypadku niespełnienia określonych wymogów Jednostka Certyfikująca NASK-PIB zawiesza udzieloną certyfikację.

7. Skargi i odwołania

118 Odwołania i skargi są rozpatrywane przez NASK-PIB z zachowaniem zasad bezstronności, poufności i uczciwości.

119 Kandydat lub osoba certyfikowana ma prawo odwołać się od decyzji w sprawie certyfikacji lub złożyć skargę do Jednostki Certyfikującej NASK-PIB.

120 Skargi i odwołania należy kierować na adres fizyczny lub elektroniczny Jednostki Certyfikującej NASK-PIB.

121 Odwołania należy składać w ciągu 14 dni od daty otrzymania decyzji w sprawie certyfikacji.

122 Tryb wnoszenia skargi lub odwołania jest opisany procedurą postępowania, wskazaną na stronie internetowej https://certyfikacja.nask.pl.

8. Stosowanie certyfikatów i logo certyfikacji

123 Osoba certyfikowana może powoływać się na certyfikację i używać logo certyfikacji (jeśli określono) tylko w odniesieniu do potwierdzonych kompetencji.

124 Nie można powoływać się na certyfikat w sposób mogący wprowadzić w błąd odbiorcę lub w zakresie innym niż objęty certyfikacją.

125 Zasady wykorzystania stosowania certyfikatów i logo certyfikacji zostały opisane na stronie internetowej https://certyfikacja.nask.pl.

126 Każde niewłaściwe stosowanie certyfikatu, jego utrata lub wprowadzające w błąd wykorzystywanie osoby certyfikowane są zobowiązane zgłosić do Jednostki Certyfikującej NASK-PIB.

127 Osoba certyfikowana nie jest uprawniona do przekazywania przyznanego jej prawa użytkowania certyfikatu osobom trzecim.

128 Osoba certyfikowana w przypadku utraty lub uszkodzenia certyfikatu, jest uprawniona do pozyskania duplikatu certyfikatu.

129 Certyfikat może być używany w takiej postaci, w jakiej został wydany i w całości. Korekty wzoru, koloru lub tekstu są niedopuszczalne.

9. Wykaz certyfikowanych osób

130 Jednostka Certyfikująca NASK-PIB prowadzi wykaz certyfikowanych osób. Wykaz ten zawiera w szczególności: identyfikację osoby certyfikowanej, termin ważności certyfikatu oraz oznaczenie dokumentu normatywnego, na zgodność z którym była przeprowadzona certyfikacja.

10. Poufność

131 Jednostka Certyfikująca NASK-PIB zobowiązuje się do zachowania poufności wszystkich informacji uzyskanych w procesie certyfikacji. Usługi na każdym etapie są świadczone w sposób bezstronny, obiektywny i etyczny. Personel własny oraz podwykonawcy zostali zobowiązani do zachowania zasad poufności w zakresie wszystkich informacji uzyskanych w procesie certyfikacji i nadzoru.

132 Informacjami poufnymi są wszelkie informacje, które wnioskujący, kandydat, osoba certyfikowana i Jednostka Certyfikująca NASK-PIB w jakiejkolwiek formie uzyskają w ramach realizacji umowy o certyfikację.

133 W przypadkach, gdy Jednostka Certyfikująca NASK-PIB jest zobowiązana poprzez odpowiednie przepisy prawne do ujawniania informacji poufnej, to wnioskujący kandydat lub osoba certyfikowana zostanie o tym poinformowany, o ile nie jest to zabronione w trybie przepisów szczególnych.

134 Do poufnych informacji uzyskanych lub wytworzonych podczas procesu certyfikacji mogą mieć również dostęp – w sytuacjach opisanych poniżej:

a) przedstawiciele Polskiego Centrum Akredytacji w zakresie niezbędnym do prowadzania oceny i nadzoru w procesie akredytacji Jednostki Certyfikującej NASK-PIB;

b) osoby fizyczne i prawne świadczące usługi na rzecz Jednostki Certyfikującej NASK-PIB na podstawie umów zapewniających zachowanie poufności, na warunkach nie mniej rygorystycznych niż określone w niniejszym dokumencie.

135 Prawo do przetwarzania informacji poufnych jest udzielone przez wnioskującego, kandydata lub osobę certyfikowaną na okres niezbędny do zrealizowania opisanych powyżej czynności.

136 Wszelkie prawa własności intelektualnej zawarte w dokumentach certyfikacyjnych wytworzonych przez Jednostkę Certyfikującą NASK-PIB pozostają jej własnością.

11. Zasady etyki postępowania przez osoby certyfikowane

137 Osoba certyfikowana wykorzystuje zdobytą wiedzę i umiejętności w ramach działań związanych z zarządzaniem podmiotami KSC zgodnie z celami organizacji.

138 Osoba certyfikowana nie wykorzystuje kompetencji potwierdzonych certyfikatem w jakikolwiek sposób, który byłby sprzeczny z prawem lub przynosiłby szkodę organizacji.

139 Osoba certyfikowana nie angażuje się świadomie w działalności, które mogą zdyskredytować dobre imię organizacji lub Jednostki Certyfikującej NASK-PIB.

140 Osoba certyfikowana jest zobowiązana do poinformowania Jednostki Certyfikującej NASK-PIB o sprawach, które mogłyby mieć wpływ na jej zdolność do dalszego spełniania wymagań certyfikacyjnych.

141 Osoba certyfikowana kieruje się najlepszymi praktykami rynkowymi i przestrzega zasad uczciwej konkurencji.

12. Opłaty

142 Wnioskujący jest zobowiązany pokryć koszty certyfikacji zgodnie z zawartą umową, niezależnie od jej wyników. Opłaty za certyfikację są określone w cenniku umieszczonym na stronie internetowej https://certyfikacja.nask.pl.