Program certyfikacji Audytorów Wiodących ISO 27001

Aktualizacja procedury / Historia zmian:	**w dniu:**	**przez:**
Opracowanie dokumentu	10.04.2019	AW/PU
Aktualizacja dokumentu	07.06.2019	PU
Zamknięcie NZ + uwzględnienie SPP	04.10.2019	PU
Usunięcie z Programu punktu związanego z opłatami	06.12.2019	PU

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

1. Wstęp

Niniejszy program certyfikacji osób, zgodnie z procedurą nr V-09SS-x03pl _Przebieg procesu certyfikacji osób, obejmuje opis certyfikacji na Audytora Wiodącego ISO 27001.

Rozwój nowych technologii oraz ich wykorzystania w każdym aspekcie życia rodzi coraz większe zapotrzebowanie na właściwe zabezpieczenia danych i informacji. Obecnie mamy do czynienia z sytuacją, kiedy nie dziwi już informacja o kolejnym przypadku ataku hakerskiego, wycieku danych wrażliwych, czy też innym incydencie naruszającym bezpieczeństwo informacji w firmie, instytucji publicznej czy innej organizacji.

Bez względu na to jakiego rodzaju informacji i danych dotyczy incydent, tj. danych osobowych, czy danych związanych z wiedzą organizacji (know-how); bez względu na fakt, czy organizacja padła ofiarą działań zamierzonych czy niezamierzonych, rośnie świadomość istotności analizy potencjalnych ryzyk i właściwego zabezpieczenia informacji.

Jeśli dodatkowo weźmiemy pod uwagę fakt, że przedmiotowy incydent może dotyczyć podmiotu o szczególnym znaczeniu dla ciągłości i bezpieczeństwa funkcjonowania Państwa, kwestia właściwego zarządzania bezpieczeństwem informacji nabiera dodatkowego znaczenia.

Krajowy system cyberbezpieczeństwa, oparty na założeniach Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii został wprowadzony ustawą z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa. Ustawodawca w ramach systemu przewidział rozwiązania i mechanizmy, obejmujące np. działania prewencyjne i kontrolne, mające na celu zapewnienie bezpieczeństwa między innymi dla operatorów usług kluczowych, dostawców usług cyfrowych i innych organizacji kluczowych z punktu widzenia funkcjonowania państwa.

W przypadku operatorów usług kluczowych za kluczowe uznano wdrożenie odpowiedniej dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do utrzymania infrastruktury kluczowej, prowadzenie systematycznej analizy ryzyka, monitorowanie incydentów, czy też wdrożenie odpowiednich dla szacowanego ryzyka zabezpieczeń technicznych i organizacyjnych.

Żeby zapewnić efektywność i jakość wdrożonych rozwiązań, ustawodawca wdrożył mechanizmy kontrolne, tj. obowiązkowe audyty bezpieczeństwa systemu informacyjnego. Miarą istotności tych audytów dla systemu cyberbezpieczeństwa jest też precyzyjne wskazanie przez ustawodawcę podmiotów, których kwalifikacje i doświadczenie powinny zwiększać gwarancję bezpieczeństwa systemów informacyjnych.

Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 roku w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu wskazuje między innymi certyfikat **audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001** wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób, jako jeden z dopuszczalnych w ramach systemu dokumentów poświadczających kwalifikacje audytującego.

Obecnie rynek oferuje wiele szkoleń, niestety o niejednolitej jakości, z zakresu systemu zarządzania bezpieczeństwem informacji. Niemniej jednak tylko dzięki restrykcyjnym wymaganiom wobec jakości takich form kształcenia oraz weryfikacji zdobytej wiedzy w drodze

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

egzaminu prowadzonego przez niezależną, akredytowaną jednostkę certyfikującą, możemy mieć realny wpływ na faktyczny poziom cyberbezpieczeństwa.

DEKRA Certification Sp. z o.o. posiada ponad 16-letnie doświadczenie w obszarze certyfikacji. Program certyfikacji został opracowany i jest monitorowany przy udziale ekspertów z przedmiotowego zakresu. Rozumiejąc znaczenie kompetentnych kadr dla bezpieczeństwa informacyjnego, dość restrykcyjnie określono kryteria dla kandydatów na audytorów wiodących, ale też dla samych egzaminatorów. Kompetentni egzaminatorzy i doświadczony personel jednostki certyfikującej czuwają nad prawidłowym przebiegiem procesu.

Założenie 3 letniej ważności certyfikatu i konieczności jego odnowienia dla utrzymania poświadczenia kwalifikacji, zobowiązuje audytorów do stałego doskonalenia umiejętności, co zapewnia trwałość wymagań i potwierdzenie rzetelności procesu certyfikacji.

Zweryfikowane kadry, zajmujące się bezpieczeństwem informacji, przyczynią się do realnego zwiększenia tego bezpieczeństwa, minimalizując ryzyko wystąpienia poważnych incydentów w tym obszarze, tak istotnych z punktu widzenia bezpieczeństwa krajowego.

2. Skróty i terminologia

- Certyfikat - dokument wydany przez JCO zgodnie z postanowieniami normy PN-EN ISO/IEC 17024:2012, wskazujący, że wymieniona osoba spełnia wymagania certyfikacyjne
- ISO 27001 – standard ISO określający wymagania dla systemu zarządzania bezpieczeństwem informacji
- Menedżer ds. Usług Ochrony Danych – pracownik JCO odpowiedzialny za prowadzenie i nadzorowanie procesów związanych ze świadczonymi usługami certyfikacji osób
- Wnioskodawca/kandydat – osoba ubiegająca się o certyfikat, która spełnia wyspecyfikowane warunki wstępne certyfikacji
- Egzaminator – osoba posiadająca kompetencje do przeprowadzenia i podania oceny wyników egzaminu, gdy w ramach tego egzaminu wymagany jest profesjonalny osąd;
- Kompetencja - zdolność wykorzystania wiedzy i umiejętności do osiągnięcia zamierzonych wyników
- Ocena – proces porównania spełniania przez wnioskodawcę wymagań zawartych w programie certyfikacji
- Odwołanie – wystąpienie wnioskodawcy o ponowne rozpatrzenie negatywnej decyzji podjętej w procesie certyfikacji
- Pomocnik egzaminatora – pracownik JCO, przeszkolony z zasad przeprowadzania egzaminów
- Proces certyfikacji - działania, łącznie z wnioskowaniem, oceną, decyzją w sprawie certyfikacji, nadzorem, ponownej certyfikacji i wykorzystaniem certyfikatów oraz logo/znaków, za pomocą których jednostka certyfikująca ustala, że dana osoba spełnia wymagania certyfikacyjne.
- Program certyfikacji - określone wymagania certyfikacyjne i zasady prowadzenia tego procesu odnoszące się do kategorii osób, w stosunku do których stosuje się te same normy i zasady oraz te same procedury
- System certyfikacji – ogół procedur i zasobów do prowadzenia procesu certyfikacji

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

LA ISO 27001	Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg PN-EN ISO/IEC 27001
JCO	Jednostka Certyfikująca Osoby
DEKRA Certification	DEKRA Certification Sp. z o.o.
VA	Procedura
AA	Instrukcja
GF	Zarząd firmy
MSR	Pełnomocnik ds. zarządzania
MR	Menedżer Regionalny
MOD	Menedżer ds. Usług Ochrony Danych
OWCO	Ogólne Warunki Certyfikacji Osób

Terminy “audit” i “audyt” oraz “auditor” i “audytor” są równoważne.

3. Powołania Normatywne

PN-EN ISO/IEC 17024:2012 Ocena zgodności. Ogólne wymagania dotyczące jednostek certyfikujących osoby.

PN-ISO/IEC 27006:2016-12 Technika informatyczna. Techniki bezpieczeństwa. Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji.

PN-EN ISO/IEC 27001:2017-6 Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.

4. Zakres stosowania

Niniejszy program certyfikacji ma zastosowanie w procesie certyfikacji wnioskodawców na Audytorów Wiodących ISO 27001. Określają one wymagania zgodne z obowiązującymi przepisami, normami i specyfikacjami w ramach zakresu akredytacji, których spełnienie jest niezbędne na poszczególnych etapach procesu.

5. Opis procesu certyfikacji

Opis pracy i zadań LA ISO 27001

Przeprowadzenie audytów systemów zarządzania bezpieczeństwem informacji, które obejmują przegląd dokumentacji, zaplanowanie, przeprowadzenie i sporządzenie raportu z audytu.

W szczególności do zadań audytora wiodącego należą:

1. Zainicjowanie audytu, w tym kontakt z przedstawicielem audytowanego
2. Przegotowanie działań audytowych, w tym:
   - Przeprowadzenie przeglądu dokumentacji
   - Przygotowanie planu audytu
   - Przedzielenie prac zespołowi audytującemu
   - Przygotowanie dokumentów roboczych
3. Przeprowadzenie działań audytowych, w tym:
   - Przeprowadzenie spotkania otwierającego i zamykającego
   - Komunikowanie się podczas audytu/ sterowanie zespołem audytowym
   - Zbieranie i weryfikowanie dowodów audytowych
   - Opracowanie ustaleń z audytu
   - Przygotowanie i prezentacja wniosków z audytu
4. Przygotowanie raportu z audytu.
5. Zakończenie audytu.
6. Przeprowadzenie działań poaudytowych – jeśli ma zastosowanie.

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

Wniosek o certyfikację osób

Proces certyfikacji rozpoczyna się w momencie złożenia w JCO przez kandydata wniosku o certyfikację osób. Do wniosku wnioskodawca powinien dołączyć kopię dokumentu poświadczającego ukończenie szkolenia w zakresie przedmiotowym certyfikacji. Wraz ze złożeniem wniosku kandydat przesyła ponadto podpisane Ogólne Warunki Certyfikacji Osób (OWCO).
Pierwszym etapem oceny jest weryfikacja złożonego wniosku przez MOD.
MOD, bądź osoba przez niego wyznaczona, sprawdza kompletność wniosku i załączników oraz prawidłowość ich wypełnienia (ocena formalna). Po sprawdzeniu kompletności wniosku i weryfikacji informacji w nim zawartych, MOD dokonuje kwalifikacji wnioskodawcy poprzez sprawdzanie spełnienia przez wnioskodawcę wymagań (ocena merytoryczna).
W procesie kwalifikacji kandydatów MOD może zwrócić się do Komitetu Technicznego o wydanie opinii.

Po pozytywnym zakwalifikowaniu wnioskodawcy, MOD bądź osoba wyznaczona dokonuje rejestracji kandydata w bazie i zakłada teczkę osobową wnioskodawcy. Wnioskujący otrzymuje potwierdzenie przyjęcia wniosku o certyfikację osób z kwalifikacją.
W przypadku negatywnego wyniku sprawdzenia MOD może wezwać wnioskującego o uzupełnienie brakujących dokumentów, bądź zawiadamia wnioskującego o nieścisłościach. Rejestracja wnioskodawcy w bazie następuje w dniu usunięcia nieścisłości.
Wniosek o certyfikację osób, wraz z załącznikami stanowi umowę pomiędzy wnioskodawcą a JCO na przeprowadzenie procesu certyfikacji.

Wymagania względem wnioskodawców, a następnie ocena i decyzja o przyznaniu certyfikatu odnosi się wyłącznie do procesu certyfikacji.

Wymagania dla wnioskodawców ubiegających się o certyfikat LA:
- ma wykształcenie wyższe techniczne lub przeszedł edukację na poziomie równoważnym wykształceniu wyższemu;
- co najmniej 4 lata pracował na pełnym etacie w instytucjach zajmujących się techniką informatyczną, z czego co najmniej 2 lata pełnił lub wykonywał funkcje związane z bezpieczeństwem informacji (pełnienia funkcji Pełnomocnika/Menadżera/Specjalisty ds. bezpieczeństwa informacji/Audytora wewnętrznego ISO 27001 lub podobnej).
- lub co najmniej **4 lata** pracował na pełnym etacie w instytucjach zajmujących się techniką informatyczną, z czego co najmniej **2 lata** w ramach obszaru doradztwa/szkoleń w zakresie bezpieczeństwa informacji).
- z sukcesem ukończył pięciodniowe (40h) szkolenie, którego zakres obejmował audyty SZBI i zarządzanie audytem lub ukończone studia podyplomowe w obszarze bezpieczeństwa informacji – w zakresie odpowiadającym ramowemu programowi szkolenia JCO.
Poza powyższymi wymaganiami JCO nie stawia żadnych dodatkowych wymagań np. dotyczących przynależności do stowarzyszeń oraz innych utrudniających dostęp do egzaminu.

Ocena

Zasadniczym etapem oceny jest egzamin sprawdzający kompetencje i wiedzę wnioskodawcy.

Egzamin składa się z części pisemnej i ustnej.
Na potrzeby egzaminów tworzona jest pula pytań egzaminacyjnych. Pula pytań przechowywana jest w sposób uniemożliwiający niepowołany dostęp do puli osób trzecich.

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

MOD minimum raz w roku i każdorazowo w przypadku zmiany wymagań prawnych dokonuje przeglądu i aktualizacji puli pytań. Nadzór nad egzaminem prowadzi Egzaminator oraz pomocnik egzaminatora/lub egzaminator nadzorujący.
Egzamin pisemny składa się z 30 pytań wielokrotnego wyboru i trwa 45 minut. Maksymalna liczba punktów do uzyskania z tej części egzaminu wynosi 30 punktów.
Aby zdać egzamin, uczestnik musi uzyskać z części testowej minimum 65% odpowiedzi poprawnych.
Egzamin ustny następuje wprost po egzaminie pisemnym. Uczestnik musi odpowiedzieć na 2 pytania punktowane łącznie do maksymalnie 20 punktów. Czas egzaminu ustnego obejmuje 20 minut na przygotowanie odpowiedzi i 10 minut na samą odpowiedź na pytania.
Aby zdać egzamin, uczestnik musi uzyskać z części ustnej minimum 65% odpowiedzi poprawnych.

Egzaminy są przeprowadzane w odpowiednich salach, zorganizowanych w sposób zapewniający indywidualne odpowiadanie na pytania. Egzaminator otrzymuje zestawy pytań w zapieczętowanej kopercie i otwiera je dopiero po ogłoszeniu reguł egzaminacyjnych.

Oceny wyników dokonuje Egzaminator w sposób uczciwy, miarodajny i wiarygodny.
Egzamin pisemny oceniany jest poprzez przyznawanie:

a) W części pisemnej - 1 punktu za poprawnie udzieloną odpowiedź i 0 za odpowiedź nieprawidłową. Za odpowiedź poprawną na pytanie testowe uważa się odpowiedź, w której zaznaczono prawidłową odpowiedź/prawidłowe odpowiedzi. Brak odpowiedzi również skutkuje uzyskaniem 0 punktów.
b) W części ustnej – maksymalnie 10 punktów za poprawną analizę problemu i udzielenie odpowiedzi na każde z pytań (łącznie maksymalnie 20 punktów). Brak odpowiedzi również skutkuje uzyskaniem 0 punktów.

Kryteria oceny pytań otwartych:

Ocena prezentacji, łącznie 10 punktów

1. Zrozumienie sytuacji w odniesieniu do obowiązków Audytora Wiodącego (zasady audytowania , komunikacja interpersonalna, zarządzanie procesem i zespołem audytu) - max. 2 punkty:

   0 pkt – brak lub bardzo ograniczona znajomość zasad audytowania, wypowiedź niekomunikatywna, zdający nie jest w stanie właściwie przedstawić roli Audytora Wiodącego w procesie audytu.

   1 pkt – zadawalająca znajomość zasad audytowania, swobodny i przejrzysty sposób prezentacji wyników zadania, zdający właściwie identyfikuje rolę Audytora Wiodącego w procesie audytu.

   2 pkt - biegła znajomość zasad audytowania, swobodny, przejrzysty dostosowany do odbiorcy sposób prezentacji wyników zadania, zdający właściwie identyfikuje rolę Audytora Wiodącego w procesie audytu również w sytuacjach złożonych.

2. Ocena wiedzy w zakresie przyporządkowania sytuacji do wymagań normy. Możliwe uzupełnienie o przyporządkowanie do wytycznych, wymagań prawnych - max. 2 punkty

   0 pkt – brak znajomości wymagań normy w odniesieniu do sytuacji. Brak odwołania do wytycznych, wymagań prawnych.

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

0,5 pkt – ograniczona znajomość wymagań normy w odniesieniu do sytuacji. Błędne odwołania do wytycznych, wymagań prawnych Zdający ma kłopoty z właściwą interpretacją wymagań normy i często potrzebuje pomocy egzaminującego.

0,75 pkt - zadawalająca znajomość wymagań normy w odniesieniu do sytuacji. Zadawalające odwołania do wytycznych, wymagań prawnych. Zdający czasami potrzebuje pomocy egzaminującego.

1 pkt – biegła znajomość wymagań normy w odniesieniu do sytuacji. Właściwe odwołania do wytycznych, wymagań prawnych. Zdający biegle interpretuje wymagania normy.

3. Ocena wiedzy w odniesieniu do aktualnego stanu techniki, który może mieć związek z bezpieczeństwem informacji - max 1 punkt :

   0 pkt – brak znajomości aktualnych rozwiązań technologicznych w zakresie bezpieczeństwa informacji .

   0,5 pkt – ograniczona znajomość aktualnych rozwiązań technologicznych w zakresie bezpieczeństwa informacji .

   0,75 pkt – zadawalająca znajomość rozwiązań technologicznych w zakresie bezpieczeństwa informacji.

   1 pkt – biegła znajomość rozwiązań technologicznych w zakresie bezpieczeństwa informacji.

4. Ocena zastosowania wiedzy w odniesieniu do działalności biznesowej/sektorowej audytowanego obszaru (adekwatność biznesowa/sektorowa w odniesieniu do ryzyk, kompletność zabezpieczeń wg ISO/IEC 27002. podatności, zagrożeń, ryzyk szczątkowych) max 1 punkt:

   0 pkt – brak umiejętności zastosowania wiedzy w doniesieniu do działalności biznesowej/sektorowej audytowanego obszaru. Wypowiedzi są nieadekwatne w odniesieniu do specyfiki audytowanego obszaru.

   0,5 pkt –ograniczona umiejętność zastosowania wiedzy w doniesieniu do działalności biznesowej/sektorowej audytowanego obszaru . Wypowiedzi sa przeważnie nieadekwatne w odniesieniu do specyfiki audytowanego obszaru.

   0,75 pkt – poprawna umiejętność zastosowania wiedzy w doniesieniu do działalności biznesowej/sektorowej audytowanego obszaru . Wypowiedzi są czasami nieadekwatne w odniesieniu do specyfiki audytowanego obszaru.

   1 pkt – biegła umiejętność zastosowania wiedzy działalności biznesowej/sektorowej audytowanego obszaru. Wypowiedzi są adekwatne w odniesieniu do specyfiki audytowanego obszaru.

5. Zrozumienie sytuacji w odniesieniu do problemów związanych z akceptacją systemu ze strony pracowników i kadry kierowniczej - max 2 punkty:

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

0 pkt – brak lub bardzo ograniczone zrozumienie sytuacji w odniesieniu do problemów związanych z akceptacją systemu ze strony pracowników i kadry kierowniczej . Zdający potrzebuje znacznej pomocy ze strony egzaminującego.

1 pkt – poprawne zrozumienie sytuacji w odniesieniu do problemów związanych z akceptacją systemu ze strony pracowników i kadry kierowniczej . Zdający potrzebuje nieznacznej pomocy ze strony egzaminującego.

2 pkt – właściwe zrozumienie sytuacji w odniesieniu do problemów związanych z akceptacją systemu ze strony pracowników i kadry kierowniczej. Zdający nie potrzebuje pomocy ze strony egzaminującego.

6. Wyjaśnienie/uzasadnienie sposobu postępowania/prawidłowość i kompletność rozwiązania problemu - max 3 punkty:

   0 pkt – zdający nie potrafi lub błędnie uzasadniania sposobu postepowania, wskazuje rozwiązanie a wypowiedzi są nieadekwatne.

   1 pkt – zdający w ograniczony sposób uzasadniania sposobu postepowania, wskazuje rozwiązanie, a wypowiedzi są przeważnie nieadekwatne.

   2 pkt – zdający zadawalająco uzasadniania sposobu postępowania, wskazuje rozwiązanie a wypowiedzi są czasami nieadekwatne.

   3 pkt - zdający biegle i kompleksowo uzasadniania sposobu postępowania, wskazuje rozwiązanie, a wypowiedzi są adekwatne.

Decyzja

Decyzję o certyfikacji podejmowana jest na podstawie:
- zatwierdzonego przez MOD wniosku o certyfikację osób;
- dokumentów egzaminacyjnych.

Przebieg procesu podejmowania decyzji o certyfikacji opisany jest w procedurze V-09SS-x03pl Przebieg procesu certyfikacji osób.

Certyfikat wydawany jest na okres 3 lat. Certyfikat powinien zawierać co najmniej:
a) imię i nazwisko osoby, która uzyskała dany certyfikat;
b) datę uzyskania certyfikatu;
c) datę upływu okresu ważności certyfikatu;
d) zakres certyfikacji;
e) nazwę jednostki certyfikującej;
f) numer identyfikacyjny;
g) podpisy osób reprezentujących jednostkę certyfikującą.
h) powołanie się na program certyfikacji łącznie z identyfikacją wydania.

Decyzje o wyniku procesu certyfikacji przekazywane są wnioskującemu pisemnie.

Od decyzji Komitetu Technicznego przysługuje wnioskującemu odwołanie, zgodnie z V-013-x01pl Odwołania i skargi – postępowanie.

JCO na wniosek posiadacza certyfikatu, dwa miesiące przed upływem ważności certyfikatu może udzielić nowego certyfikatu na kolejne trzy lata, po weryfikacji dokumentacji, wskazującej

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

na spełnienie wymagań dotyczących utrzymania kompetencji. Warunkiem ponownej certyfikacji jest:

- przedłożenie dokumentów świadczących o tym, że posiadacz certyfikatu podwyższał w okresie ważności certyfikatu swoje kwalifikacje w dziedzinie związanej z zakresem działalności objętej certyfikatem, poprzez przedstawienie zaświadczeń ze szkoleń z wymagań prawnych lub wymagań odpowiedniej normy w wymiarze co najmniej 8 godzin, a także dowody potwierdzające przeprowadzenie co najmniej 3 zewnętrzne audyty SZBI z co najmniej 6 dniami audytu na miejscu lub co najmniej 6 wewnętrznych audytów SZBI z co najmniej 12 dniami audytu na miejscu w okresie posiadania certyfikatu.
- brak zasadnych skarg na poziom wiedzy i umiejętności posiadacza certyfikatu oraz nie przekraczanie i nie nadużywanie uprawnień wynikających z certyfikatu,

w okresie ważności certyfikatu.
Odnowienie certyfikatu następuje po 3 latach.

Cofnięcie certyfikatu

DEKRA Certification Sp. z o.o. jako Jednostka Certyfikująca Osoby uprawniona jest w każdym momencie do cofnięcia certyfikatu DEKRA, jeżeli:

- warunki przyznania certyfikatu nie są (już) spełnione, na przykład ze względu na podanie niekompletnych lub nieprawdziwych danych w procedurze certyfikacyjnej;
- nie zostały spełnione wymagania postawione przez jednostkę certyfikacyjną w okresie zawieszenia certyfikatu kompetencji
- wystąpią inne przyczyny uprawniające do cofnięcia certyfikatu na podstawie OWCO.

W przypadku cofnięcia certyfikatu, uzyskanie certyfikatu wymaga ponownej certyfikacji.

Zawieszenie certyfikatu

DEKRA Certification Sp. z o.o. uprawniona jest w każdym momencie do zawieszenia certyfikatu DEKRA w przypadku:

- zgłoszenia przez osobę certyfikowaną czasowej rezygnacji z certyfikatu
- gdy osoba certyfikowana lub zleceniodawca, tj. podmiot delegujący pracownika do procesu certyfikacji, nie dopełniają obowiązków nałożonych na nich w związku z certyfikacją, na przykład obowiązku informowania o zmianach, lub nie spełniają zobowiązań wynikających z umowy zawartej z DEKRA Certification Sp. z o.o. w szczególności zobowiązań dotyczących płatności;
- gdy przedmiot użytkowania, na przykład certyfikat DEKRA, wykorzystywany będzie niezgodnie z warunkami użytkowania, określonymi w OWCO;
- stwierdzenia przekroczenia uprawnień, wynikających z przyznanego certyfikatu lub mających na celu świadome wprowadzenie w błąd

- niespełnienia wymagań określonych przez jednostkę certyfikującą, stwierdzonego w okresie ważności certyfikatu.

6. Prawa i obowiązki wnioskodawcy i osoby certyfikowanej

Kandydat do certyfikacji ma prawo do:
- żądania wglądu do dokumentacji z przebiegu swojego procesu certyfikacji.
- wniesienia skargi/odwołania na przebieg procesu certyfikacji po otrzymaniu decyzji z każdego etapu procesu
- oceny egzaminu i egzaminatora
- złożenia zastrzeżenia do osoby egzaminatora (przed egzaminem)
- rezygnacji z przystąpienia do egzaminu
- korzystania z dozwolonych pomocy podczas egzaminu (norma ISO 27001).

Kandydat do certyfikacji ma obowiązek:
- zastosowania się do przedstawionych warunków przeprowadzania egzaminu
- samodzielnej pracy podczas egzaminu.

Osoba certyfikowana zobowiązana jest do spełniania warunków przyznania certyfikatu i do niezwłocznego informowania DEKRA Certification o wszelkich zmianach mogących mieć wpływ na spełnienie warunków utrzymania certyfikatu.

7. Prawa i obowiązki JCO

Obowiązkiem JCO jest sprawowanie nadzoru nad prawidłowością stosowania certyfikatu.
JCO zobowiązana jest do powiadamiania posiadacza certyfikatu o zmianach w systemie certyfikacji oraz zmianach przepisów prawnych i norm dotyczących certyfikatu w okresie jego ważności. Zmiany te będą przesyłane posiadaczom certyfikatów w formie informacji drogą elektroniczną.

JCO ma obowiązek przechowywać i nadzorować dokumentację dotyczącą wnioskodawcy i osoby certyfikowanej, a także dokumentację z przebiegu certyfikacji, w warunkach zapewniających ochronę danych, bezpieczeństwo i poufność.

Jednostka certyfikująca przechowuje i nadzoruje, dokumentację dotyczącą każdej osoby, która otrzymała certyfikat oraz dokumentację z przebiegu procesu certyfikacji.
Dokumentacja dotycząca poszczególnych osób jest przechowywana w warunkach zapewniających bezpieczeństwo i poufność. Dane dotyczące przebiegu procesu certyfikacji i nadzoru rejestrowane są również w bazie.

8. Wymagania dla jednostek szkoleniowych (trenerzy, programy szkoleniowe, organizacja)

DEKRA Certification nie prowadzi szkoleń z zakresu objętego programem certyfikacji.

Jednostka prowadząca szkolenia dla AW ISO 27001 powinna wyznaczyć osobę odpowiedzialną za ogólne zarządzanie szkoleniami, która będzie czuwała nad jakością świadczonych usług szkoleniowych oraz kompetencjami trenerów.
Jednostka prowadząca szkolenia dla AW ISO 27001 powinna ponadto mieć określone wymagania kompetencyjne dla trenerów.
Ponadto jednostka powinna zapewnić monitorowanie jakości prowadzonych szkoleń.

Obowiązkiem jednostki prowadzącej szkolenia dla AW ISO 27001 jest zapewnienie uczestnikom szkoleń informacji o warunkach uczestnictwa w szkoleniu, programie szkolenia i kwestiach organizacyjnych.

Jednostka prowadząca szkolenia powinna prowadzić dokumentację z przeprowadzonych szkoleń wraz z rejestrem wydanych Zaświadczeń ze szkolenia.

Program szkolenia powinien określać m.in. cel szkolenia, jego zakres tematyczny, oraz jego plan. Program szkolenia musi być zgodny z programem określonym przez JCO – załącznik nr 1 do Umowy z firma szkoleniową. Każdy uczestnik szkolenia powinien otrzymać pełen zestaw materiałów szkoleniowych.

Uznane przez DEKRA Certification jednostki szkoleniowe wymienione są na naszej stronie internetowej.

Jednocześnie JCO akceptuje wnioski wnioskodawców, którzy ukończyli szkolenia w innych jednostkach szkoleniowych pod warunkiem, że szkolenie to spełnia warunki ramowego programu szkolenia AW ISO 27001 DEKRA Certification.

9. Kwalifikacje i powołanie egzaminatorów

Wszyscy egzaminatorzy są powoływani przez Zarząd DEKRA Certification lub przez MOD.
Powoływanie egzaminatorów w DEKRA Certification odbywa się w oparciu o przedstawione kwalifikacje oraz możliwość spełnienia określonych funkcji.
Wymagania w stosunku do egzaminatorów:

- Wykształcenie wyższe
- Doświadczenie zawodowe:

  minimum **5 lat** doświadczenia zawodowego w wymiarze **pełnego etatu organizacjach zajmujących się techniką informacyjną**, z czego **co najmniej 3 lata** pełnił lub wykonywał funkcje związane z bezpieczeństwem informacji; (pełnienia funkcji Pełnomocnika/Menadżera/Specjalisty ds. bezpieczeństwa informacji/Audytora wewnętrznego ISO 27001 lub podobnej).

  lub minimum **5 lat** doświadczenia zawodowego w wymiarze **pełnego etatu organizacjach zajmujących się techniką informacyjną**, z czego **co najmniej 3 lata** w ramach obszaru doradztwa/szkoleń w zakresie bezpieczeństwa informacji).

  oraz udokumentowane przeprowadzenie **min. 4 audytów certyfikacyjnych, z tego co najmniej 20 dni na miejscu w audytowanej organizacji** . Udział powinien obejmować wstępne określenie zakresu i planowanie, przegląd dokumentacji i szacowania ryzyka, ocenę wdrożenia i opracowanie formalnego raportu z audytu.

- Ukończone szkolenia/kursy audytowania SZBI, zarządzanie audytem oraz bezpieczeństwa i ochrony informacji w wymiarze łącznym **co najmniej 40 godzin lub ukończone studia podyplomowe w bezpieczeństwa informacji** – w zakresie odpowiadającym ramowemu programowi szkolenia JCO.

- Ukończone szkolenie w zakresie aktualnych wymagań normatywnych związanych z Programem certyfikacji LA ISO 27001 (w tym także ISO 17024).

Warunkiem nawiązania współpracy z egzaminatorem jest podpisanie dokumentu D-06S-x09pl Warunki przeprowadzania egzaminów w ramach certyfikacji osób.

Powołanie na egzaminatora udzielane jest na 3 lata, na podstawie wypełnionego profilu zawodowego. W tym czasie obowiązkowo musi być przeprowadzony przynajmniej 1 monitoring egzaminatora. Powołanie może zostać przedłużone na kolejne trzy lata. Warunkiem utrzymania statusu egzaminatora jest przeprowadzenie przez niego min. 1 egzaminu oraz pozytywna ocena z monitoringu, dokonanego przez MOD lub osobę przez niego wyznaczoną.

W czasie trwania powołania, egzaminator jest zobowiązany raz w roku uczestniczyć w wymianie doświadczeń dla egzaminatorów. Ponadto egzaminator zobowiązany jest do odbycia co najmniej jednego szkolenia/kursu w wymiarze 8 godzin lub udziału w konferencji o tematyce bezpieczeństwa informacji.

Na 3-4 miesiące przed datą wygaśnięcia ważności powołania Egzaminator jest informowany o upływie jego ważności. Egzaminator proszony jest o przesłanie zaktualizowanego profilu zawodowego wraz z załącznikami o utrzymaniu kwalifikacji.
Wznowienie powołania następuje najpóźniej na 4 tygodnie przed upływem daty ważności poprzedniego powołania - data ważności poprzedniego powołania zostaje przedłużona o kolejne 3 lata.

W czasie trwania powołania na egzaminatora przynajmniej raz musi być dokonana ocena przeprowadzenia egzaminu. Oceny egzaminatora dokonuje MOD lub osoba przez niego wyznaczona

Szczegółowa procedura powoływania egzaminatorów znajduje się w dokumencie V-09SS-x03pl Przebieg procesu certyfikacji osób.

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

10. Załączniki

- Załącznik 1 – umowa z firmą szkoleniową:

Umowa nr …….

zawarta w dniu …….... pomiędzy:

DEKRA Certification Sp. z o.o. z siedzibą we Wrocławiu, , ul. Legnicka 48H

54-202 Wrocław

wpisaną do Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Wrocławia-Fabrycznej, VI wydział Gospodarczy; numer KRS 0000010810;

NIP 899-24-08-842, którą reprezentują:

1.

2.

zwaną dalej **DEKRA Certification,**

a

……..

z siedzibą w …….., wpisaną do Krajowego Rejestru Sądowego w Sądzie ……. pod numerem KRS …….

którą reprezentuje:

……

zwaną dalej Jednostką szkoleniową

§ 1 Postanowienia ogólne

1. Przedmiotem umowy jest ustalenie zasad i warunków współpracy pomiędzy DEKRA Certification a Jednostką szkoleniową.
2. Strony deklarują współpracę w zakresie propagowania idei podnoszenia i potwierdzania kwalifikacji osób poprzez certyfikację.
3. Umawiające się strony nie są upoważnione do przekazywania praw i obowiązków wynikających z tej umowy na podmioty trzecie, bez wcześniejszej pisemnej zgody drugiej strony.
4. Strony nie mają prawa żądania od siebie wzajemnie jakiegokolwiek wynagrodzenia z tytułu realizacji niniejszej umowy.

§ 2 Zobowiązania stron

1. Jednostka szkoleniowa przygotuje materiały szkoleniowe dla kandydatów do certyfikacji oraz programy szkolenia zgodnie z ramowymi wytycznymi, ujętymi w załączniku nr 1 do niniejszej umowy.

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

2. Jednostka szkoleniowa jest organizatorem szkoleń otwartych realizowanych w ramach niniejszej umowy.
3. DEKRA Certification ma prawo wglądu do programu i materiałów, o których mowa w ust. 1 przed podpisaniem niniejszej umowy oraz po każdej zmianie dokonanej w tych programach i materiałach. Ponadto Jednostka szkoleniowa zobowiązuje się udostępnić program i materiały na każde żądanie DEKRA Certification. Ograniczenie możliwości wglądu może być podstawą rozwiązania niniejszej umowy.
4. DEKRA Certification dopuszcza do egzaminów kandydatów, którzy odbyli szkolenie w Jednostce szkoleniowej według programów i z udziałem materiałów, o których mowa w ust. 1 i 3, pod warunkiem spełniania przez tych kandydatów pozostałych wymagań dopuszczających do udziału w egzaminie.
5. DEKRA Certification przeprowadza egzaminy w oparciu o program certyfikacji w zakresie, którego dotyczą szkolenia, opisane w załączniku.
6. Jednostka szkoleniowa zobowiązuje się do zlecania prowadzenia szkoleń, określonych w załączniku nr 1 wyłącznie ekspertom o wysokich kwalifikacjach, gwarantujących wysoki poziom prowadzonych szkoleń, wpisanym do bazy kwalifikowanych trenerów-ekspertów Jednostki szkoleniowej
7. DEKRA Certification i Jednostka szkoleniowa zobowiązują się do zachowania w tajemnicy wszystkiego, co wiąże się ze wzajemną współpracą w ramach niniejszej umowy, w szczególności przekazanych materiałów i informacji oraz treści niniejszej umowy. Zobowiązanie to obowiązuje w czasie trwania Umowy i po jej zakończeniu. Na stronach ciąży zobowiązanie do tego samego swoich pracowników.
8. Strony wyrażają zgodę na przekazanie materiałów marketingowych swoim klientom, w szczególności broszur informacyjnych dotyczących ich działalności.

§ 3 Zawiązanie i rozwiązanie Umowy

1. Umowa wchodzi w życie z dniem jej podpisania przez obydwie strony.
2. Umowę zawarto na czas nieokreślony.
3. Każdej ze stron przysługuje prawo rozwiązania umowy w każdym czasie za wypowiedzeniem. Okres wypowiedzenia wynosi 3 miesiące.
4. W przypadku naruszenia postanowień niniejszej umowy każda ze stron ma prawo rozwiązać umowę w trybie natychmiastowym, bez zachowania okresu wywiedzenia, po uprzednim pisemnym wezwaniu drugiej strony do zaprzestania naruszeń w terminie 7 dni i niezastosowaniu się przez drugą stronę do powyższego wezwania.
5. Umowa może być rozwiązana przez każdą ze stron ze skutkiem natychmiastowym, bez zachowania okresu wypowiedzenia w przypadkach:
    a. dokonania zmian w programach i materiałach szkoleniowych o których mowa w §2 ust. 1 i 3 bez pisemnego poinformowania i akceptacji DEKRA Certification,
    b. naruszenia zasad dotyczących konkurencji,
    c. złamania zasady zachowania tajemnicy,
    d. narażenia dobrego imienia lub wizerunku jednej ze stron Umowy,
    e. niedotrzymania warunków określonych w Umowie.
6. Wypowiedzenie umowy nie zwalnia stron z obowiązku ukończenia prac, zleceń i wywiązania się ze zobowiązań podjętych przed dokonaniem wypowiedzenia

przez jedną ze stron, w szczególności w sytuacji, gdy zobowiązania te dotyczą osób i podmiotów trzecich.

7. Rozwiązanie umowy pomiędzy stronami nie ma wpływu na ważność wystawionych przez DEKRA Certification certyfikatów i zaświadczeń.
8. W przypadku wypowiedzenia umowy przez którąkolwiek ze stron, strony zobowiązane są do zwrotu wszystkich powierzonych wzajemnie wydawnictw, materiałów roboczych, metodologii i innej dokumentacji. Strony nie mają prawa do wykonywania jakichkolwiek kopii, magazynowania na nośnikach magnetycznych, systemach komputerowych i innych, a także do przekazywania innym osobom, instytucjom, etc. ww. dokumentów.

§ 4 Postanowienia końcowe

1. Podpisanie niniejszej umowy przez strony unieważnia wszelkie wcześniejsze ustalenia poczynione w jakiejkolwiek formie.
2. Strony zobowiązują się do rozstrzygania wszystkich sporów w sposób polubowny.
3. Sądem miejscowo właściwym dla rozstrzygania sporów wynikających z umowy jest sąd właściwy dla siedziby DEKRA Certification.
4. Niniejsza umowa może zostać zmieniona przez strony z zachowaniem formy pisemnej pod rygorem nieważności.
5. Strony nie dokonały żadnych ubocznych ustaleń ustnych zmieniających treść niniejszej umowy.
6. Do rozwiązania niniejszej umowy wystarczy przesłanie listem poleconym stosownego pisma. Jako wiążącą uznaje się datę stempla pocztowego.
7. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

....

DEKRA Certification Sp. z o.o.

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/

Zał. Nr 1 do umowy nr ……..

Jednostka prowadząca szkolenia:

- wyznacza osobę odpowiedzialną za ogólne zarządzanie szkoleniami, która będzie czuwała nad jakością świadczonych usług
- określa wymagania kompetencyjne dla trenerów
- monitoruje jakość prowadzonych szkoleń
- prowadzi dokumentacje ze szkoleń wraz z rejestrem uczestników
- prowadzi szkolenia odpowiadające ramowemu programowi:

Ramowy Program szkolenia dla Audytorów Wiodących ISO 27001.

LP	TEMAT	Czas teoria (h)	Czas ćwiczenia/dyskusja(h)
1.	Wymagania normy PN-ISO/IEC 27001:2017	12	28
2.	Bezpieczeństwo informacji		
3.	Wymagania prawne i regulacyjne istotne dla bezpieczeństwa informacji		
4.	Szacownanie ryzyka oraz zarządzanie ryzykiem		
5.	ISO 19011 i odpowiednie fragmenty ISO / IEC 17021, ISO / IEC 27006 i ISO / IEC 27007		
6.	Metodyka audytu		
7.	Planowanie audytów i programów audytu		
8.	Przeprowadzanie audytów		
9.	Techniki komunikacji		
10	Radzenie sobie z krytycznymi sytuacjami audytu		
11	Audyty w praktyce		
12	Kontynuacja audytów		
13	Ocena wyników audytu		
14	Określenie i śledzenie działań korygujących		
15	Przygotowywanie raportów z audytu		
16	Kompetencje i ocena audytorów		
	RAZEM:	12	28

DEKRA Certification Sp. z o.o., ul. Legnicka 48 H, 54-202 Wrocław, Telefon: 71/780 47 77, Fax: 71/780 47 79, www.dekra-certification.com.pl/