

Nr zapytania 12/2026

Opis przedmiotu zamówienia – Część I



na usługę pn.:

„Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), opracowanie i wdrożenie Systemu Zarządzania Ciągłością Działania (SZCD), przeprowadzenie audytów cyberbezpieczeństwa, organizacja i przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa w ramach projektu „Wzmocnienie cyberodporności sieci IT i OT oraz ciągłości działania w Zakładzie Wodociągów i Kanalizacji Sp. z o.o. Świecie poprzez wdrożenie kluczowych środków technicznych oraz rozwój kompetencji.”

Świecie, dnia: 15.07.2026 r.

Zatwierdza:
Prezes



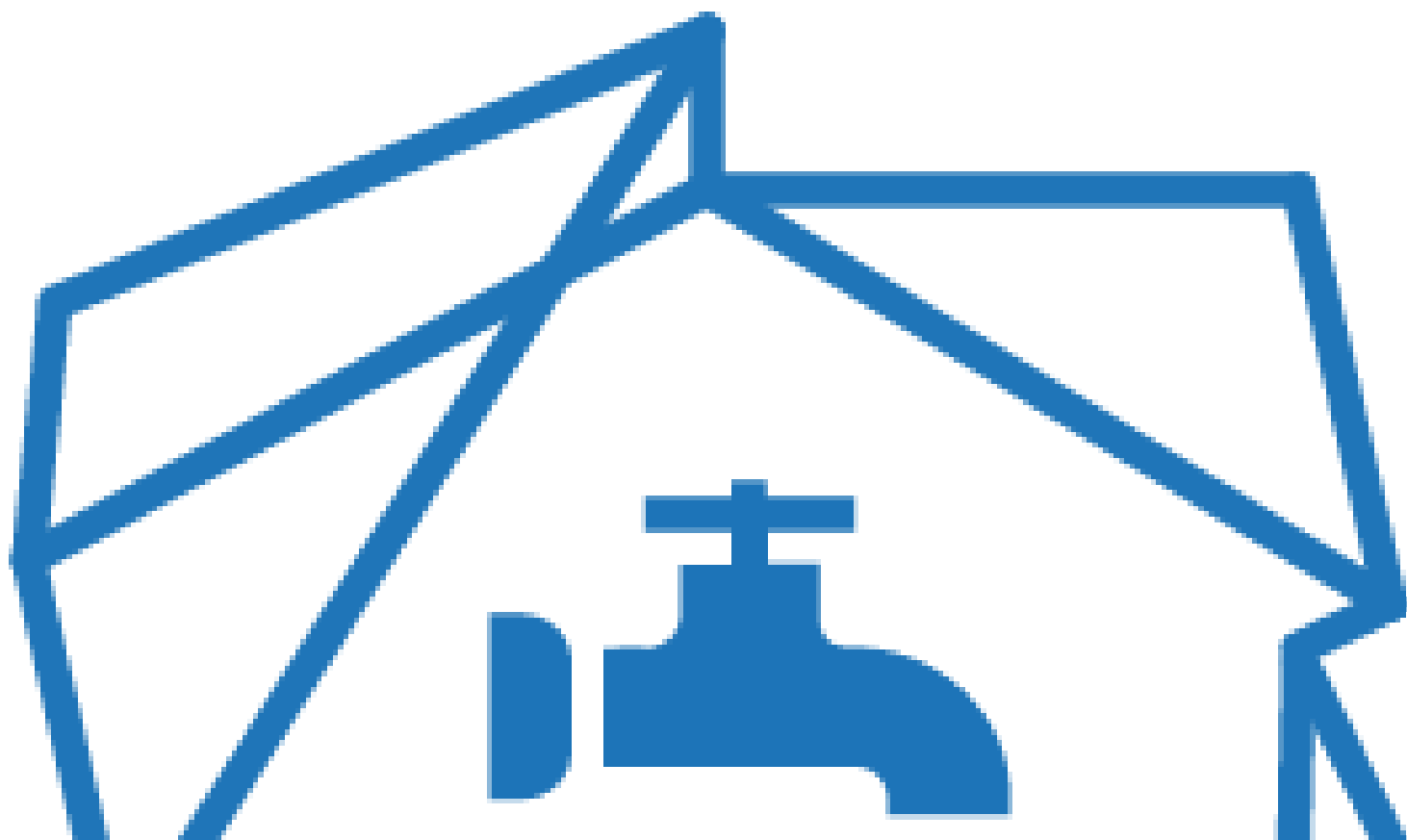
Signed by /
Podpisano przez:

Andrzej Kozłowski

Date / Data: 2026-
07-15 14:36

Spis treści

Obszar organizacyjny – Dokumentacja.....	3
U20. Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI);.....	3
U23. Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Ciągłością Działania STI (SZCD)	4
Obszar organizacyjny - Audyty	6
U25. Audyt SZBI, audyt SZCD, audyt zgodności KRI/uokSC przez wykwalifikowanych audytorów, audyt (re)certyfikacji SZBI, SZCD na zgodność z normami IT/OT/ICS	6
Obszar kompetencyjny – szkolenia Wszystkie szkolenia mają odbyć się w siedzibie zamawiającego	7
U26. Szkolenia z zakresu cyberbezpieczeństwa - podstawowe szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników IT/OT/ICS	7
U27. Szkolenia z zakresu cyberbezpieczeństwa – szkolenia dla kadry, istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji IT/OT/ICS.....	8
U29. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami IT/OT/ICS	9
Oprogramowanie – aplikacja do zarządzania dokumentacją.....	17



1. Postanowienia ogólne i zakres OPZ

Niniejszy Opis Przedmiotu Zamówienia (dalej: „OPZ”) określa minimalne wymagania Zamawiającego dla Części I, która łączy obszar organizacyjny i kompetencyjny:

- Obszar organizacyjny – Dokumentacja (opracowanie, wdrożenie, przegląd i aktualizacja SZBI oraz SZCD);
- Obszar organizacyjny – Audyty (audyt zgodności KRI/UoKSC, audyt SZBI i SZCD);
- Obszar kompetencyjny – Szkolenia (szkolenia z zakresu cyberbezpieczeństwa oraz dostęp do platformy szkoleniowej).

Wykonawca zobowiązany jest zrealizować pełen zakres wybranej części. Szczegółowe warunki udziału w postępowaniu, podstawy wykluczenia oraz wymagane podmiotowe środki dowodowe (w tym wymagania dotyczące kwalifikacji zawodowej i organizacyjnej Wykonawcy) określone zostały w treści Zapytania ofertowego (pkt 5) i nie są powielane w niniejszym OPZ.

Obszar organizacyjny – Dokumentacja

U20. Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI);

1. Wykonawca jest zobowiązany do wykonania audytu przedwdrożeniowego oraz opracowania u Zamawiającego kompleksowej dokumentacji SZBI, obejmującej polityki, procedury, instrukcje mające na celu zarządzanie ryzykiem związanym z bezpieczeństwem informacji.
2. Dokumentacja powinna kompleksowo uwzględniać aspekty związane z bezpieczeństwem fizycznym, w tym środki ochrony dedykowane pomieszczeniom, urządzeniom, infrastrukturze technicznej oraz personelowi, minimalizujące ryzyko wynikające z zagrożeń fizycznych, takich jak nieautoryzowany dostęp, kradzież czy inne incydenty. Dodatkowo, dokumentacja powinna obejmować kwestie związane z bezpieczeństwem technologicznym, skoncentrowane na zabezpieczeniu systemów teleinformatycznych przed potencjalnymi zagrożeniami, oraz bezpieczeństwem organizacyjnym i osobowym, uwzględniającym procedury operacyjne, szkolenia pracowników oraz polityki ochrony danych.
3. SZBI musi być dopasowany do realiów operacyjnych Zamawiającego oraz charakterystyki jego systemów IT i OT. Przeprowadzone musi zostać również szacowanie ryzyka (na podstawie ISO/IEC 27005), obejmujące inwentaryzację aktywów, identyfikację zagrożeń i podatności, ocenę prawdopodobieństwa i skutków oraz opracowanie planu postępowania z ryzykiem.
4. SZBI musi obejmować minimum następujące obszary:
 - a) ustanowienie polityki bezpieczeństwa informacji oraz polityk tematycznych,
 - b) aktualizacji regulacji wewnętrznych w zakresie bezpieczeństwa informacji,
 - c) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji,
 - d) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,
 - e) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia,
 - f) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji,
 - g) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
 - h) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
 - i) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie,

- j) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
- k) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży,
- l) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych,
- m) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji,
- n) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

5. Dokumentacja musi uwzględniać wymagania następujących aktów prawnych oraz norm:

- a) Norma PN-EN ISO/IEC 27001:2023;
- b) Norma PN-EN ISO/IEC 27002:2023;
- c) 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;
- d) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

6. Wykonawca ma obowiązek przekazać Zamawiającemu:

- pełną dokumentację systemu zarządzania bezpieczeństwem informacji;
- zalecenia mające na celu zwiększenie poziomu bezpieczeństwa informacji Zamawiającego.

Wykonawca zapewni bieżące wsparcie merytoryczne dla zespołu wdrożeniowego w trakcie całego procesu wdrażania systemu. Konsultacje będą odbywać się w dni robocze, od poniedziałku do piątku, za pośrednictwem bezpiecznych kanałów komunikacji, takich jak rozmowy telefoniczne, korespondencja emailowa, telekonferencje lub bezpośrednie spotkania w siedzibie Zamawiającego.

U23. Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Ciągłością Działania STI (SZCD)

1. Wykonawca jest zobowiązany do opracowania dla Zamawiającego systemu zarządzania ciągłością działania, obejmującego polityki, procedury, działania, role, kompetencje i procesy mające na celu zapewnić ciągłość działania organizacji w przypadku wystąpienia zakłóceń.
2. SZCD musi być dopasowany do realiów operacyjnych Zamawiającego oraz charakterystyki jego systemów IT i OT.
3. SZCD musi objąć:
 - a) kontekst organizacji,
 - b) politykę ciągłości działania,
 - c) cele ciągłości działania,
 - d) zdefiniowanie wymaganych kompetencji i umiejętności personelu,
 - e) zasady komunikacji z zainteresowanymi stronami,
 - f) analizę wpływu biznesowego,
 - g) szacowanie ryzyka,
 - h) zasady monitorowania i oceny SZCD,
 - i) program audytów wewnętrznych,
 - j) zasady zarządzania niezgodnościami i działaniami korygującymi,
 - k) strategię ciągłości działania,
 - l) scenariusze incydentów,

m) plany i procedury ciągłości działania systemów IT i OT.

4. W pierwszym kroku musi zostać wykonana audyt przedwdrozeniowy względem wymagań Rozporządzenia KRI oraz ustawy o krajowym systemie cyberbezpieczeństwa, aby precyzyjnie określić braki organizacyjne, kompetencyjne i techniczne oraz ustalić priorytety i harmonogram działań.

5. W ramach przygotowania SZCD Wykonawca zobowiązany jest do uwzględnienia różnych rodzajów zagrożeń i scenariuszy, takich jak:

- a) cyberataki i pracę awaryjną w trakcie przełączania się z głównej infrastruktury ICT na nadmiarowe zdolności,
- b) częściowe lub całkowite awarie obiektów biurowych i lokali,
- c) częściowe lub całkowite awarie ośrodków przetwarzania danych,
- d) niedostępność krytycznej liczby pracowników lub członków personelu odpowiedzialnych za zagwarantowanie ciągłości operacji,
- e) wpływ klęsk żywiołowych,
- f) wpływ ataków fizycznych, w tym włamań i ataków terrorystycznych,
- g) ataki wewnętrzne,
- h) przerwy w dostawie energii elektrycznej na szeroką skalę.

6. Dokumentacja musi uwzględniać wymagania następujących aktów prawnych oraz norm: •

- a) Norma PN-EN ISO/IEC 22301;
- 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.

7. Wykonawca ma obowiązek przekazać Zamawiającemu:

- pełną dokumentację systemu zarządzania ciągłością działania;
- zalecenia mające na celu zwiększenie poziomu bezpieczeństwa informacji Zamawiającego.

8. Wykonawca zapewni bieżące wsparcie merytoryczne dla zespołu wdrożeniowego w trakcie całego procesu wdrażania systemu. Konsultacje będą odbywać się w dni robocze, od poniedziałku do piątku, za pośrednictwem bezpiecznych kanałów komunikacji, takich jak rozmowy telefoniczne, korespondencja e-mailowa, telekonferencje lub bezpośrednie spotkania w siedzibie Zamawiającego.

9. System powinien obejmować całościowe podejście – od prewencji po reakcję na zakłócenia i wyciąganie wniosków z incydentów.

Obszar organizacyjny - Audyty

U25. Audyt SZBI, audyt SZCD, audyt zgodności KRI/uoKSC przez wykwalifikowanych audytorów, audyt (re)certyfikacji SZBI, SZCD na zgodność z normami IT/OT/ICS

Przedmiotem zamówienia jest usługa wykonania audytu zgodności, którego kryterium jest 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 (zwanym dalej „Rozporządzeniem KRI”) oraz Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (zwana dalej „UoKSC”).

Audyt musi być przeprowadzony przez co najmniej trzech audytorów posiadających uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

Audyt musi być zrealizowany w siedzibie Zamawiającego, w wymiarze co najmniej 1 dnia roboczego (tj. 8 godzin).

Audyt ma obejmować weryfikację bezpieczeństwa fizycznego (sprawdzenie ochrony pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp), bezpieczeństwa informatycznego (analiza bezpieczeństwa systemu teleinformatycznego) oraz bezpieczeństwa organizacyjnego i osobowego (stosowane procedury bezpieczeństwa), w tym przegląd dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji.

Audyt musi obejmować weryfikację:

- 1 systemu zarządzania bezpieczeństwem informacji,
- 2 zapewnienia aktualizacji regulacji wewnętrznych w zakresie bezpieczeństwa informacji,
- 3 utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji,
- 4 przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,
- 5 podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia,
- 6 zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji,
- 7 zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
- 8 ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
- 9 zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie,
- 10 zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
- 11 ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży,
- 12 zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych,
- 13 bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji,
- 14 zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Kryteriami audytu są:

- a) 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;
- b) Ustawa o Krajowym Systemie Cyberbezpieczeństwa;
- c) Norma ISO/IEC 27001; • Norma ISO 22301; • Dyrektywa NIS 2.

Wykonawca zobowiązany jest do dostarczenia Zamawiającemu:

- a) rekomendacji do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego,
- b) raportu z audytu.

Obszar kompetencyjny – szkolenia

Wszystkie szkolenia mają odbyć się w siedzibie zamawiającego

U26. Szkolenia z zakresu cyberbezpieczeństwa - podstawowe szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników IT/OT/ICS

1. Szkolenia pracowników muszą obejmować co najmniej tematykę:

- Podstawowych zasad cyberhigieny;
- Typów ataków wraz z przykładami;
- Reagowania na incydenty;
- Odpowiedzialności prawnej.

2. W ramach szkolenia, uczestnicy muszą otrzymać konkretne porady do zastosowania w praktyce, tak aby możliwe było ich sprawne i zarazem bezpieczne funkcjonowanie w cyberprzestrzeni. Program kursu musi skupiać się na najważniejszych w danym obszarze aspektach. Trenerzy muszą zapewnić wysoki poziom merytoryczny oraz komunikacyjny. Szkolenie ma zapoznać uczestnika z zagrożeniami, technikami ataków cyberprzestępczych oraz metodami socjotechnicznymi, ukierunkowanymi na osoby pracujące na co dzień przed komputerem. Uczestnicy mają dowiedzieć się jak działa rynek cyberprzestępczy, jakimi kwotami operują współcześni przestępcy, jakimi sposobami próbują uzyskać dostęp do sieci teleinformatycznej oraz jak w czasie rozmowy osobistej, telefonicznej lub mailowej oszuści potrafią wyłudzić informację od nieświadomego pracownika. Podczas szkolenia uczestnik ma być również edukowany ze skutków, dla których wykorzystywanie komputera służbowego do celów prywatnych zwiększa ryzyko ataku na całą organizację.

3. Szkolenie musi być skierowane do każdego pracownika w organizacji bez względu na jego wiedzę i umiejętności informatyczne.

4. Korzyści po szkoleniu:

- a) zdobycie wiedzy obejmującej bezpieczne zarządzanie miejscem pracy oraz danymi;
- b) zdobycie wiedzy umożliwiającej ochronę przed atakami socjotechnicznymi.

5. Wykonawca zobowiązany jest do:

- a) wydania imiennych certyfikatów dla każdego uczestnika,
- b) zapewnienia dla każdego uczestnika materiałów szkoleniowych w formie elektronicznej.

6. Wymiar szkolenia: 2 godziny na turę.

7. Szczegółowa tematyka szkolenia dla pracowników:

- Wprowadzenie do bezpieczeństwa informacji
- Atrakcyjność ofiar
- Czy cyberprzestępczość się opłaca?
- Aktualne trendy w zakresie cyberbezpieczeństwa
- Aktualne zagrożenia związane z sytuacją geopolityczną
- Rodzaje ataków cybernetycznych
- Analiza faz ataków
- Oszustwa płatnicze
- Przykłady ataków ukierunkowanych
- Spoofing telefoniczny i sms-owy
- Sztuczna inteligencja, a cyberbezpieczeństwo
- Jak postępować kiedy staniemy się ofiarą?
- Zasady postępowania z danymi uwierzytelniającymi
- Fałszywe strony WWW
- Ataki z wykorzystaniem kodów QR
- Największe wycieki danych w Polsce
- Ataki na systemy przemysłowe
- Sztuczki cyberprzestępców
- Podstawy ataków socjotechnicznych
- Jak bronić się przed socjotechniką?
- Zasady higieny w cyberprzestrzeni
- Aspekty bezpieczeństwa fizycznego

U27. Szkolenia z zakresu cyberbezpieczeństwa – szkolenia dla kadry, istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji IT/OT/ICS

1. W ramach realizacji usługi Wykonawca przeprowadzi szkolenia dla zespołu ds. SZBI, powołanego przez Zamawiającego, w którym omówione zostaną zasady funkcjonowania i utrzymania systemu zarządzania bezpieczeństwem informacji (SZBI).
2. Szkolenie z wdrażania udokumentowanego Systemu Zarządzania Bezpieczeństwem Informacji przygotowuje do zarządzania bezpieczeństwem w oparciu o normę ISO 27001, obejmując analizę kontekstu organizacji, szacowanie ryzyka, wybór i wdrażanie zabezpieczeń, tworzenie dokumentacji (polityk, procedur, instrukcji), a także audytowanie i ciągłe doskonalenie systemu w celu ochrony informacji przed zagrożeniami, zgodnie z wymaganiami prawnymi.
3. Główne cele szkolenia:
 - Zrozumienie wymagań normy ISO/IEC 27001 - dogłębna analiza punktów normy, terminologii, celów bezpieczeństwa informacji, zasad przywództwa, planowania i funkcjonowania SZBI;
 - Praktyczne umiejętności - nauka identyfikacji aktywów informacyjnych, analizy i oceny ryzyka (np. metodą PDCA), projektowania i wdrażania zabezpieczeń;
 - Tworzenie dokumentacji - ćwiczenia z tworzenia polityki bezpieczeństwa, procedur, instrukcji i deklaracji stosowania.
 - Rola pełnomocnika ds. SZBI oraz audytora wewnętrznego - wyjaśnienie roli koordynatora lub pełnomocnika SZBI, a także audytorów wewnętrznych.
 - Aspekty prawne i organizacyjne - uwzględnienie wymagań prawnych (np. dyrektywy NIS 2), kontekstu organizacji, oczekiwań interesariuszy oraz roli zasobów ludzkich.

4. Minimalny program szkolenia:

- Wprowadzenie - definicje, zakres SZBI, rola dokumentacji (polityki, procedury);
- Kontekst organizacji - analiza otoczenia, identyfikacja interesariuszy;
- Przywództwo - wymagania dla kierownictwa;
- Planowanie - ustalanie celów, podejście oparte na ryzyku;
- Wsparcie - zasoby, kompetencje, komunikacja, dokumentacja;
- Funkcjonowanie - realizacja procesów, identyfikacja i ocena ryzyka;
- Ocena wyników - monitorowanie, pomiary, audyty wewnętrzne;
- Doskonalenie - działania korygujące i zapobiegawcze.
- Zabezpieczenia organizacyjne, osobowe, fizyczne i technologiczne
- Ćwiczenia praktyczne - identyfikacja ryzyka, tworzenie i przegląd dokumentów.

5. Wymiar szkolenia: co najmniej 4 godziny zegarowe na turę.

U29. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami IT/OT/ICS

Szkolenie obejmuje kompleksowe przygotowanie personelu organizacji do rozpoznawania i reagowania na zagrożenia socjotechniczne, ze szczególnym uwzględnieniem ataków phishingowych w różnych formach. Program łączy dwa wzajemnie uzupełniające się elementy: weryfikację rzeczywistego poziomu świadomości pracowników poprzez kontrolowane symulacje ataków oraz ustrukturyzowane szkolenie podnoszące kompetencje w zakresie cyberbezpieczeństwa.

Szkolenie adresowane jest przede wszystkim do specjalistów posiadających zdefiniowane obowiązki w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), jednak obejmuje również szerszy krąg pracowników mających dostęp do systemów IT, OT oraz ICS. Celem jest nie tylko przekazanie wiedzy teoretycznej, ale przede wszystkim wykształcenie właściwych nawyków i odruchów reakcji w sytuacji rzeczywistego zagrożenia - zgodnych z przyjętymi w organizacji procedurami bezpieczeństwa.

1. Przeprowadzenie kampanii phishingowej oraz przygotowanie raportu zawierającego wyniki z analizą kampanii:

- wybór domeny (tudząco podobnej do prawdziwych domen Zamawiającego), która zostanie wykorzystana do kampanii phishingowej;
- opracowanie bazy mailingowej pracowników objętych kampanią phishingową oraz spreparowanego dokumentu zbliżonego wyglądem do dokumentów Zamawiającego, zawierającego dodatkowy niezłśliwy kod pozwalający na mierzenie efektów kampanii;

- wyznaczenie osób wtajemniczonych w fakt przeprowadzania testów (np. najwyższe kierownictwo, dział informatyczny lub wyłącznie szef tego działu, inspektor ochrony danych lub inna osoba odpowiedzialna za bezpieczeństwo w organizacji);
- dodanie domeny wybranej do przeprowadzenia kampanii phishingowej do tzw. białej/zaufanej listy w celu pominięcia filtrów antyspamowych (celem testu jest dostarczenie spreparowanej wiadomości na wszystkie skrzynki pracowników i weryfikacja ich podatności na prawdziwe kampanie cyberprzestępców);
- przeprowadzenie kampanii phishingowej (wysłanie przygotowanej uprzednio wiadomości e mail do pracowników wskazanych w bazie mailingowej)
- raport z testu phishingowego

2. Testy muszą być zrealizowane w wymiarze co najmniej 7 dni roboczych (tj. 16 godzin).

3. Przeprowadzenie prób ataków socjotechnicznych polega na wywieraniu wpływu na ludzi i stosowaniu perswazji w celu oszukania ich tak, aby uwierzyli, że socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji, tożsamości. Dzięki temu socjotechnik jest w stanie wykorzystać swoich rozmówców, przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji. Przeprowadzane próby w Organizacji miały na celu zweryfikowanie świadomości pracowników i zabezpieczeń przed atakami socjotechnicznymi.

4. Testy muszą składać się z następujących faz:

- Rozpoznanie (biały wywiad, obserwacja pracy pracowników).
- Budowanie więzi i zaufania (użycie wewnętrznych informacji, podawanie się za kogoś innego, wspomnianie nazwisk osób znanych ofierze, zgłoszenie potrzeby pomocy lub zasugerowanie posiadania władzy).
- Wykorzystanie zaufania (prośba o informację lub działanie skierowana do ofiary).

5. Zakres testów:

- Ataki typu phishing,
- Ataki typu spear phishing
- Phishing typu whaling
- Phishing przez klonowanie
- Angler phishing

6. Wykonawca zobowiązany jest do wykrycia (w stosunku do konkretnego adresu email):

- otwieranych wiadomości,
- otwierania plików w popularnych formatach, takich jak „docx.”, czy „xlsx”,
- otwieranych stron za pomocą linków umieszczonych w wiadomościach,
- podawanych poświadczeń na stronach mających na celu wyłudzenie informacji, przygotowanych przez testerów.

Dostęp do platformy

W ramach szkoleń wykonawca dostarczy dostęp do platformy szkoleniowej online na okres do końca kwalifikowalności –31.12.2026 – w celu ugruntowania wiedzy dostarczanej na szkoleniach.

Minimalne wymagania dotyczące platformy:

Lp	Platforma szkoleniowa
1.	Nieograniczony jednoczesny dostęp dla 40 użytkowników do 31.12.2026r.
2.	Użytkownicy mają dostęp do wsparcia technicznego, a także do ekspertów, którzy mogą pomóc w rozwiązywaniu trudnych kwestii związanych z materiałem kursu.
3.	Kursy dostosowane są do różnych poziomów zaawansowania i potrzeb użytkowników.
4.	Materiały szkoleniowe aktualizowane są co najmniej raz na kwartał zgodnie z najnowszymi trendami i wytycznymi w zakresie cyberbezpieczeństwa.
5.	Szkolenia dostępne są w języku polskim.
6.	Szkolenia obejmują zapoznanie uczestników z przykładami ataków cybernetycznych oraz metodami obrony przed tymi atakami.
7.	W ramach szkolenia, uczestnicy otrzymują konkretne porady do zastosowania w praktyce, tak aby możliwe było ich sprawne i zarazem bezpieczne funkcjonowanie w cyberprzestrzeni. Program kursu musi skupiać się na najważniejszych w danym obszarze aspektach.

8.	Szkolenia dostępne są z poziomu przeglądarki internetowej za pośrednictwem Internetu.
9.	Szkolenia zawierają testy o ustalonych progach zdawalności oraz quizy z losowym wybieraniem pytań z puli.
10.	Certyfikaty potwierdzające zdobycie wiedzy wydawane są po ukończeniu każdego z kursów.
11.	Wiedza przekazywana jest przy pomocy różnorodnych sposobów: praktyczne zadania, nagrania wideo itd.
12.	Poszczególne etapy nauki utrwalane są za pomocą zróżnicowanych zadań.
13.	Platforma umożliwia śledzenie postępów w nauce.
14.	Uczestnicy mogą używać platformy do partycypowania w kursach, przesyłania zadań, rozwiązywania quizów, przeglądania udostępnionych materiałów.
15.	Platforma umożliwia automatyczne dzielenie uczestników na grupy.
16.	Możliwe są samodzielne zapisy do kursów (również w sposób zautomatyzowany).
17.	Możliwe jest tworzenie ankiet ewaluacyjnych, raportów ze szkoleń i ich składowych oraz eksport ich wyników do arkuszy kalkulacyjnych.

18.	Pogłębiony panel raportów i analiz pozwala na ewaluację następujących danych: aktywni użytkownicy; zapisy na kurs i wskaźnik ukończenia kursu; postęp kursu; popularne kursy; statystyki certyfikatów; użytkownicy w czasie rzeczywistym; codzienna aktywność; lista nieaktywnych użytkowników.
19.	Platforma oferuje całą gamę narzędzi komunikacyjnych. Zaimplementowane są między innymi: czat, forum, tablica ogłoszeń, komunikaty i powiadomienia e-mail.
20.	Użytkownicy mogą na platformie wybierać kursy zgodnie ze swoimi potrzebami, tworząc indywidualne ścieżki rozwoju.
21.	Kursy są wzbogacone o interaktywne elementy, takie jak quizy, zadania praktyczne, studia przypadków, które ułatwiają zrozumienie skomplikowanych zagadnień.
22.	Platforma jest dostępna o każdej porze dnia i nocy, co pozwala na naukę w dogodnym dla użytkownika momencie, bez konieczności dostosowywania się do sztywnych harmonogramów.
23.	System pozwala na śledzenie postępów w nauce, co motywuje do regularnej pracy i osiągania kolejnych etapów szkolenia.
24.	Każdy kurs zakończony jest testem wiedzy, a po jego zdaniu uczestnik otrzymuje certyfikat potwierdzający zdobyte kompetencje.

	Kursy:
25.	Szkolenie z podstaw cyberbezpieczeństwa dla pracowników
26.	Szkolenie dla kadry zarządzającej z zakresu cyberbezpieczeństwa
	Zakres tematyczny:
27.	Wstęp do cyberbezpieczeństwa
28.	W jakim czasie następuje pierwszy atak?
29.	Po co ktoś ma nas atakować?
30.	Czy cyberprzestępczość się opłaca?
31.	Dane z raportów dotyczących stanu cyberbezpieczeństwa
32.	Najpopularniejsze zagrożenia
33.	Aktualne zagrożenia związane z konfliktem na Ukrainie

34.	Rodzaje ataków cybernetycznych
35.	Analiza ataków cybernetycznych
36.	Przewodnik po metodach obrony instytucji
37.	Cyberbezpieczeństwo osobiste
38.	Ataki na osoby fizyczne - co zrobić kiedy staniemy się ofiarą?
39.	Sztuczna inteligencja, a cyberbezpieczeństwo
40.	Największe wycieki danych w Polsce
41.	Ataki na systemy OT
42.	Sztuczki cyberprzestępców
43.	Podstawy ataków socjotechnicznych
44.	Jak bronić się przed socjotechniką?
45.	Zasady higieny w cyberprzestrzeni

46.	Aspekty bezpieczeństwa fizycznego
47.	Podstawy prawne w obszarze cyberbezpieczeństwa
	Wymagania bezpieczeństwa:
48.	Platforma oferuje zaawansowane funkcje bezpieczeństwa, takie jak szyfrowanie danych, wielopoziomowe uwierzytelnienie użytkowników oraz monitorowanie aktywności.
49.	Platforma poddawana jest regularnie testom bezpieczeństwa (co najmniej raz na kwartał), które identyfikują i eliminują potencjalne luki bezpieczeństwa.
50.	Serwery platformy znajdują się w data center, które spełnia najwyższe standardy bezpieczeństwa fizycznego i technologicznego. Obejmuje to zaawansowane zabezpieczenia przeciwpożarowe, kontrolę dostępu oraz systemy redundantne, które zapewniają ciągłość działania platformy.
51.	Wszystkie dane przesyłane między użytkownikiem, a platformą są szyfrowane za pomocą protokołu SSL/TLS, co zabezpiecza je przed przechwyceniem przez nieuprawnione osoby.
52.	Konieczne aktualizacje oprogramowania powinny dokonywać się automatycznie bez udziału Zamawiającego.

Oprogramowanie – aplikacja do zarządzania dokumentacją

Należy dostarczyć oprogramowanie umożliwiające zarządzanie dokumentacją.

Opis aplikacji do zarządzania dokumentacją

I. Wymagania ogólne oprogramowania

1. Oprogramowanie ma być dostarczone w najnowszej wersji w języku polskim.
2. Oprogramowanie powinno posiadać dokumentację użytkownika opisującą funkcjonalność każdego z modułów oprogramowania oraz dokumentację administratora opisującą sposób administrowania programem w tym jego instalowania, konfiguracji, sposobu tworzenia kopii zapasowych oraz odtwarzania w przypadku awarii,
3. Program powinien umożliwiać pracę zarówno na komputerach stacjonarnych jak i na urządzeniach mobilnych np. smartfonach.
4. Program na komputerze klienckim powinien posiadać możliwość instalacji jako aplikacja PWA.
5. Koszt zakupu oprogramowania powinien uwzględniać koszt wszystkich składników oprogramowania (poza systemem operacyjnym zainstalowanym na serwerze Zamawiającego), które są niezbędne do jego pracy zgodnie z niniejszą specyfikacją.
6. W ramach zamówienia Zamawiający otrzyma wersję instalacyjną oprogramowania oraz licencję uprawniającą do korzystania z przedmiotowego oprogramowania.
7. Dostawca do końca roku 2026 licząc zapewnia wsparcie, w ramach którego Zamawiający zostanie uprawniony do nieodpłatnego pobierania poprawek i aktualizacji oraz na bieżąco pomocy (nadzoru) w obsłudze programu.

II. Techniczne dane oprogramowania

1. Program powinien pracować jako aplikacja intranetowa uruchamiana i prawidłowo pracująca w aktualnych wersjach przeglądarek internetowych (MS Edge, Google Chrome, FireFox).
2. Wszystkie dane gromadzone w oprogramowaniu powinny być zapisywane wyłącznie centralnie, na komputerze pełniącym rolę serwera pracującego w trybie ciągłym przez 24 godziny na dobę.
3. Serwer będzie dostarczony przez Zamawiającego i będzie znajdował się w jego siedzibie.
4. Program powinien pracować na serwerze z procesorem 8-rdzeniowy w architekturze 64 bit., min. 1TB SSD, min. 16GB RAM z zainstalowanym systemem operacyjny Windows lub Linux (inne składniki oprogramowania niezbędne do pracy programu dostarcza Dostawca).
5. Aplikacja instalowana na serwerze działającym w systemie Windows powinna posiadać automatyczny instalator wszystkich składników niezbędnych do prawidłowego działania oprogramowania.
6. Poza instalatorem dla systemu Windows aplikacja powinna mieć możliwość uruchomienia na serwerze pracującym pod systemem Linux (konfiguracja instalacji niestandardowych powinna być określona w dokumentacji programu).

7. Program ma mieć możliwość importu użytkowników z przygotowanego zgodnie ze specyfikacją pliku lub ich importu bezpośrednio z Active Directory.
8. Program ma mieć możliwość opcjonalnej integracji z Active Directory.

III. Funkcjonalność oprogramowania i jego zakres działania

1. Specjalistyczne oprogramowanie do zarządzania organizacją w tym bezpieczeństwem informacji i ochroną danych osobowych, musi posiadać funkcjonalności, które umożliwiają zarządzanie obszarami:

procesami – w tym zakresie oprogramowanie musi:

- posiadać rejestr zidentyfikowanych procesów w tym procesów z zakresu ochrony danych, który umożliwia ich podział na makroprocesy,
- posiadać możliwość opisu procesu poprzez określenie początku i końca procesu, danych wejściowych i wyjściowych procesu, dostawcę, klienta procesu, zakresu podmiotowego i przedmiotowego, dokumentów wymaganych w procesie oraz ryzyk wpływających na osiągnięcie celu procesów,
- posiadać graficzny edytor do tworzenia interaktywnych map procesów (z możliwością podpinania plików pod dowolne elementy grafu),

komórkami organizacyjnymi – w tym zakresie oprogramowanie musi:

- posiadać rejestr komórek organizacyjnych,
- posiadać możliwość opisu komórki organizacyjnej poprzez określenie jej podrzędności w strukturze organizacyjnej, przypisania do niej stanowisk pracy oraz zakresu zadań jaki realizuje,

stanowiskami pracy – w tym zakresie oprogramowanie musi:

- posiadać rejestr stanowisk pracy przypisanych do właściwych komórek organizacyjnych,
- posiadać możliwość opisu stanowiska pracy poprzez określenie m.in.: miejsca stanowiska pracy w strukturze organizacyjnej, celu istnienia stanowiska pracy, liczby podległych pracowników, głównych zadań realizowanych na stanowisku pracy, wymaganych upoważnień i pełnomocnictw obowiązujących na danym stanowisku pracy oraz wymaganiach w zakresie kompetencji czy doświadczenia,

pracownikami – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich pracowników, praktykantów i stażystów oraz osób świadczących pracę na umowach cywilnoprawnych,
- posiadać możliwość przesłania historii zatrudnienia pracownika, w zakresie m.in. obejmowanych stanowisk pracy, pełnionych przez niego funkcji i posiadanych uprawnień w aplikacjach,

dokumentami – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich dokumentów określających wymagania (m.in.: polityk, zarządzeń, decyzji, instrukcji, procedur) obowiązujących na poszczególnych stanowiskach pracy,
- posiadać możliwość opisanie dokumentu poprzez m.in.: określenie osoby odpowiedzialnej za dokument, przypisanie do procesu, który realizuje oraz wskazanie właściwych stanowisk pracy na jakich obowiązuje,
- posiadać możliwość udostępniania treści dokumentu pracownikom,
- posiadać możliwość elektronicznego wnioskowania o utworzenie bądź zmianę dokumentu, nadzorowania etapów jego tworzenia oraz opiniowania przez wytypowanych użytkowników przesłanego projektu dokumentu,
- posiadać możliwość dystrybucji zatwierdzonego dokumentu na stanowiska pracy, na których obowiązuje dokument,
- posiadać możliwość elektronicznego zapoznania się przez użytkownika, będącego jednocześnie pracownikiem Zamawiającego, z dokumentem obowiązującym na zajmowanym przez niego stanowisku pracy i elektronicznego potwierdzenia zapoznania się z treścią dokumentu,
- posiadać narzędzia weryfikacji danych dotyczących potwierdzenia zapoznania pracowników z dokumentacją obowiązującą na ich stanowisku pracy,

założeń SZBI – w tym zakresie oprogramowanie musi:

- wspomagać opisywanie kontekstu organizacji w tym dokumentować okresowe analizy czynników mających wpływ na zdolność organizacji do osiągnięcia zamierzonych celów, umożliwiać opisanie zakresu i wyłączeń systemu oraz potrzeb i oczekiwań stron zainteresowanych,
- udostępniać pracownikom przygotowaną w programie deklarację polityki bezpieczeństwa informacji wraz ze spójnymi z nią celami powiązanych z procesami oraz wskaźnikami ich pomiarów,
- w sposób przejrzysty udostępniać pracownikom organizacji pełne wymagania systemu zarządzania bezpieczeństwem informacji i ochrony danych osobowych, w tym prezentować w formie graficznej wzajemne powiązania dokumentacji (tworzyć interaktywny schemat z możliwością otwierania poszczególnych dokumentów po kliknięciu na elementy grafu).

sprzętem komputerowym i oprogramowaniem komputerowym – w tym zakresie oprogramowanie musi:

- posiadać rejestr sprzętu informatycznego oraz zainstalowanego na nim oprogramowania komputerowego,
- mieć możliwość automatycznego sczytywania parametrów sprzętowych i oprogramowania zainstalowanego na komputerach działających pod kontrolą systemu operacyjnego Windows,
- posiadać możliwość ewidencjonowania bieżących przeglądów sprzętu komputerowego oraz zainstalowanego na nim oprogramowania,

- posiadać możliwość elektronicznego zgłaszania usterek i awarii sprzętu komputerowego,
- posiadać możliwość ewidencjonowania rodzaju umów serwisowych na sprzęt komputerowy,
- posiadać możliwość ewidencjonowania i zarządzania materiałami eksploatacyjnymi niezbędnymi do pracy sprzętów komputerowych np. tonery do drukarek,
- posiadać możliwość ewidencji wszystkich zdarzeń, czynności naprawczych, serwisowych czy konserwacyjnych komputerów lub serwera.

licencjami na oprogramowanie – w tym zakresie oprogramowanie musi:

- posiadać rejestr licencji oprogramowania komputerowego zainstalowanego na komputerach oraz rejestr umów licencyjnych,
- posiadać możliwość ewidencji posiadanych przez organizację umów na korzystanie z licencji programów komputerowych,

obsługą problemów zgłaszanych przez użytkowników – w tym zakresie oprogramowanie musi:

- dostarczać użytkownikom kanał komunikacji do zgłaszania problemów z obszaru IT,
- określać kategorie zgłoszeń i ustalać osoby odpowiedzialne za ich obsługę,
- dokumentować obsługę zgłoszeń oraz nadzorować terminowości ich realizacji,
- udostępniać w postaci graficznej analizę czasu obsługi zgłoszeń.

aktywami informacyjnymi – w tym zakresie oprogramowanie musi:

- umożliwiać prowadzenie rejestru zidentyfikowanych aktywów informacyjnych oraz zasobów wspomagających,
- wspomagać opisywanie aktywów m.in. poprzez wskazanie procesów przetwarzających informacje oraz istotności informacji dla realizacji danego procesu, wskazanie zasobów wykorzystywanych przy przetwarzaniu informacji oraz określenie poziomu istotności zasobu dla informacji,
- umożliwiać ustalenie wymaganego poziomu podstawowych oraz dodatkowych atrybutów informacji i adekwatnie do tego ustalać klasyfikacje aktywów.

ochrony danych osobowych – w tym zakresie oprogramowanie musi:

- umożliwiać prowadzenie zgodnie z przepisami prawa rejestru czynności przetwarzania i kategorii czynności przetwarzania danych osobowych w organizacji,
- posiadać możliwość rejestrowania klauzul informacyjnych udostępnianych przez administratora danych osobowych, a w przypadku klauzul kierowanych do pracowników program automatycznie informuje pracowników o konieczności zapoznania się z klauzulą informacyjną i udostępnia użytkownikom uprawnionym informacje o dacie zapoznania się pracowników z poszczególnymi klauzulami informacyjnymi,

- posiadać możliwość ewidencji zawartych przez organizację umów powierzenia przetwarzania danych osobowych,
- wspomagać wystawianie upoważnień do przetwarzania danych osobowych oraz prowadzić rejestr osób upoważnionych do przetwarzania danych osobowych,
- posiadać elektroniczny rejestr udostępnionych danych osobowych, który zawiera m.in. informacje o wnioskującym, dacie wniosku, podstawie prawnej upoważniającej do udostępnienia danych, zakresie udostępnionej informacji oraz terminie i osobie udostępniającej,
- umożliwiać ewidencjonowanie oraz wspomagać obsługę wniosków wynikających z RODO tj.:
 - dostęp do danych osobowych (art. 15 RODO),
 - sprostowanie danych osobowych (art. 16 RODO),
 - usunięcie danych osobowych (art. 17 RODO),
 - ograniczenie przetwarzania danych osobowych (art. 18 RODO),
 - przeniesienie danych osobowych (art. 20 RODO),
 - sprzeciw wobec przetwarzania danych osobowych (art. 21 RODO),

zarządzaniem ryzykiem bezpieczeństwa informacji – w tym zakresie oprogramowanie musi:

- posiadać rejestr zidentyfikowanych ryzyk w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych,
- posiadać możliwość przypisania stanowiska odpowiedzialnego za zidentyfikowane ryzyko i jego cyklicznej oceny,
- posiadać możliwość identyfikacji i ewidencji czynników ryzyka (źródeł zagrożeń i szans), podatności na zagrożenia lub szanse, opisanie skutków ryzyka, estymację i ocenę ryzyka, ustalenia reakcji na ryzyko oraz monitorowania i raportowania ryzyka,
- posiadać możliwość przeprowadzania cyklicznej oceny ryzyka,
- prezentować ryzyka w formie graficznych zestawień m.in. mapy ryzyka,

zarządzania uprawnieniami użytkowników w aplikacjach – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich aplikacji użytkowanych w organizacji,
- posiadać rejestr nadanych w organizacji uprawnień do przetwarzania danych w aplikacjach komputerowych zgodnie z zakresem zadań wykonywanych przez pracownika,
- posiadać możliwość elektronicznego wnioskowania o nadanie właściwych uprawnień dla pracowników zgodnie z ich zakresem obowiązków do obsługi programów komputerowych, w których są przetwarzane dane osobowe,
- w przypadku aplikacji przetwarzających dane osobowe weryfikować czy pracownik posiada upoważnienie do przetwarzania danych osobowych,
- ustalać etapy przetwarzania wniosku m.in. akceptację, opiniowanie zatwierdzenie,

- informować użytkowników odpowiedzialnych za realizację danego etapu przetwarzania wniosku o konieczności jego zrealizowania,
- posiadać możliwość elektronicznego potwierdzenia przez pracownika zapoznania się z zakresem nadanego uprawnienia,

incydentami i słabościami systemu – w tym zakresie oprogramowanie musi:

- posiadać rejestr zaistniałych incydentów oraz słabości systemu,
- posiadać możliwość zgłoszenia zidentyfikowanego zdarzenia lub słabości systemu bezpieczeństwa informacji (w tym naruszenia ochrony danych osobowych),
- umożliwiać analizę i klasyfikację zgłoszonego zdarzenia,
- wspomagać obsługę incydentów bezpieczeństwa informacji w tym określenia operatora incyduentu oraz ewidencjonować podejmowane działania,
- posiadać stosowne zestawienia dotyczące zidentyfikowanych incydentów i słabości systemów w organizacji,

certyfikatami bezpieczeństwa – w tym zakresie oprogramowanie musi:

- posiadać rejestr certyfikatów bezpieczeństwa,
- posiadać możliwość wnioskowania o nadanie certyfikatu bezpieczeństwa,
- umożliwiać użytkownikom uprawnionym ewidencjonowanie certyfikatów bezpieczeństwa,
- umożliwiać elektroniczne potwierdzenia posiadania przez pracownika certyfikatu bezpieczeństwa,
- informować użytkowników uprawnionych o zbliżającym się terminie ważności certyfikatu i nadzorować etapy jego odnowienia,
- posiadać możliwość unieważniania certyfikatu bezpieczeństwa,

formularzami IT – w tym zakresie oprogramowanie musi:

- umożliwiać tworzenie wzorców elektronicznych formularzy w tym definiować etapy ich przetwarzania oraz pola,
- umożliwiać użytkownikom składanie formularzy IT,
- umożliwiać obsługę formularzy na poszczególnych etapach ich przetwarzania przez osoby uprawnione.

wewnętrznymi audytami w zakresie bezpieczeństwa informacji i ochroną danych osobowych – w tym zakresie oprogramowanie musi:

- posiadać rejestr przeprowadzonych w organizacji audytów wewnętrznych w tym audytów w zakresie bezpieczeństwa informacji i ochrony danych osobowych,

- posiadać możliwość tworzenia programów auditów wewnętrznych na dany rok oraz planowania auditów z określeniem m.in.: zakresu auditu, przedmiotu auditu, komórek organizacyjnych uczestniczących w działaniach auditowych, terminu przeprowadzenia auditu oraz osób przeprowadzających audit,
- możliwość dokumentowania podjętych działań auditowych tj. przygotowanie m.in.: programu auditów na dany rok, protokołu końcowego z auditu,
- możliwość dokumentowania wszystkich spostrzeżeń, niezgodności i wniosków wynikłych podczas podjętych działań auditowych,
- możliwość zgłoszenia zauważonych podczas auditu niezgodności do właściwej osoby odpowiedzialnej,

działaniami doskonalącymi – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich zidentyfikowanych w organizacji nieprawidłowości (niezgodności) w zakresie bezpieczeństwa informacji i ochrony danych osobowych,
- posiadać możliwość elektronicznego zgłaszania zidentyfikowanych nieprawidłowości w funkcjonowaniu systemu bezpieczeństwa informacji i ochrony danych osobowych,
- możliwość analizy zgłoszonej nieprawidłowości przez osoby za to odpowiedzialne,
- możliwość określenia działań korygujących i korekcyjnych względem zidentyfikowanej nieprawidłowości oraz głoszenia wykonania działań korygujących,

przeglądami zarządzania w zakresie bezpieczeństwa informacji i ochroną danych osobowych – w tym zakresie oprogramowanie musi:

- posiadać rejestr przeprowadzanych w organizacji cyklicznych przeglądów zarządzania w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych,
- możliwość automatycznego przygotowania raportu do analizy z zakresu m.in. bezpieczeństwa informacji i ochrony danych osobowych.

2. Wszystkie moduły programu muszą być ze sobą kompatybilne i wzajemnie powiązane (moduły powinny korzystać z danych wprowadzanych w innych modułach bez konieczności ponownego ewidencjonowania tych samych danych).
3. Program musi informować użytkownika o działaniach, które musi podjąć w aplikacji ze względu na posiadane w aplikacji uprawnienia lub zajmowane w organizacji stanowisko pracy.
4. Komunikaty adresowane do użytkowników muszą być dostępne po zalogowaniu użytkownika do bezpośrednio aplikacji i w formie powiadomień PUSH oraz równolegle wysyłane na adres e-mail użytkownika.
5. Z poziomu komunikatu przesłanego pocztą elektroniczną użytkownik może przejść bezpośrednio do modułu w programie, w którym musi podjąć działania.

IV. Licencja

1. Licencja ma być przyznana na czas nieograniczony.
2. Licencja ma zezwalać na jednoczesną pracę w programie wszystkich pracowników Zamawiającego.
3. Licencja nie może ograniczać liczby końcówek jednocześnie korzystających z oprogramowania.
4. Licencja musi dopuszczać tworzenie przez Zamawiającego dowolnej ilości kopii oprogramowania dla celów testowych lub szkoleniowych.

Wymagania od firmy wykonawczej – kwalifikacja zawodowa oraz organizacyjna:

W zapytaniu ofertowym w punkcie 5.3.1. Część I.

