

Zadanie: Przegląd i aktualizacja dokumentacji SZBI, szkolenia z cyberbezpieczeństwa oraz dostawa, wdrożenie i utrzymanie systemu wspomagającego proces analizy ryzyka oraz zarządzania incydentami.

Założenia ogólne

Działania realizowane są w ramach projektu dofinansowanego z funduszu UE pn.: „Podniesienie poziomu cyberbezpieczeństwa w Urzędzie Miejskim w Dąbrowie Górniczej”, zgodnie z celami Programu Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa - Cyberbezpieczny Samorząd (CS).

Słownik:

1. Ustawa KSC (uoKSC) - Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa wraz zapisami projektu nowelizacji z dnia 3 października 2024 r. ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, wraz z ewentualnymi kolejnymi zmianami projektu ustawy KSC lub wprowadzoną nowelizacją.
2. NIS2 - 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 uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).
3. RODO - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 27.04.2016 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 (Dz. Urz. UE L 2016 Nr 119, s. 1, zwanego dalej RODO), wraz z ustawą z dn. 10.05.2018 r. o ochronie danych osobowych (Dz. U. z 2019, poz. 1781 tj. z późn. zm.), a także innych ustaw szczególnych, tzw. sektorowych, czy też kodeksów branżowych dotyczących ochrony danych osobowych.
4. Usługa - pod pojęciem usługi rozumie się także zadanie publiczne realizowane przez Urząd Miejski w Dąbrowie Górniczej.
5. SZBI – System Zarządzania Bezpieczeństwem Informacji
6. Poradnik NASK - Poradnik NASK Cyberbezpieczny samorząd Warszawa 2023 – poradnik dotyczący realizacji projektów z działania 2.2 pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”.
7. JST – jednostka samorządu terytorialnego

Cele realizacji projektu:

Celem działania jest podniesienie poziomu cyberbezpieczeństwa w Urzędzie Miejskim w Dąbrowie Górniczej. Efektem działania ma być dostosowana do potrzeb organizacji zamawiającego dokumentacja SZBI. Dokumentacja ma być zgodna z obowiązującymi przepisami prawa, wymaganiami konkursu z którego dofinansowywany jest projekt, w tym w szczególności wymaganymi opisanymi w Poradniku NASK. Działania mają wspierać osiągnięcie przez zamawiającego spełnienia wymagań konkursu i mają być oparte na dobrych praktykach i zgodne z najnowszym stanem wiedzy w zakresie

bezpieczeństwa informacji, tworząc ład organizacyjny w tym obszarze. Podjęte działania mają zapewnić bezpieczeństwo informacji i danych osobowych oraz systemów IT, w których są one przetwarzane. Wdrożone procedury określone w SZBI, mają minimalizować ryzyko braku sprawnej i skutecznej ochrony informacji i danych osobowych oraz zapewnić zgodny z prawem, proporcjonalny i odpowiedni do potrzeb poziom bezpieczeństwa, którego osiągnięcie ma uwzględniać koszty. Zastosowane w tym celu mają zostać rozwiązania prawne, techniczne, operacyjne i organizacyjne. Efektem działań ma być wyszkolony w zakresie bezpieczeństwa informacji personel zamawiającego. Efektem działań ma być również wdrożony system informatyczny wspomagający realizację procesów wynikających z opracowanej dokumentacji SZBI w tym, w szczególności obsługujący realizację procesów analizy ryzyka oraz zarządzania incydentami.

Projekt będzie obejmował:

Zadanie 1 – Obszar organizacyjny - Przegląd i aktualizacja dokumentacji SZBI.

Zadanie 2 – Obszar kompetencyjny - Szkolenia z cyberbezpieczeństwa.

Zadanie 3 – Obszar techniczny - System wspomagający proces analizy ryzyka oraz zarządzania incydentami.

Wykonawca zrealizuje zadania w zakresie nie mniejszym niż:**Zadanie 1 – Obszar organizacyjny - Przegląd i aktualizacja dokumentacji SZBI.**

Wykonanie przeglądu i aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji wraz z Polityką Bezpieczeństwa Informacji Urzędu Miejskiego w Dąbrowie Górniczej zgodnie z poniższymi wymaganiami:

Wdrożenie wymagań bezpieczeństwa informacji zgodnie z wymaganiami dyrektywy NIS2 oraz zapisami Ustawy KSC oraz RODO w tym w szczególności:

1. Przeprowadzenie audytu otwarcia (GAP Analysis) w celu identyfikacji różnic (luki) między aktualnym stanem organizacji, dokumentacji i procesów, a stanem pożądanym, zgodnym z Ustawą KSC oraz NIS2 i RODO. Weryfikacja działania procesów związanych z ochroną bezpieczeństwa informacji, cyberbezpieczeństwem oraz RODO, w tym w szczególności procesów analizy ryzyka, zarządzania incydentami, zarządzania ciągłością działania, procesów związanych z RODO, procesu zarządzania upoważnieniami dopuszczającymi. Przygotowanie raportu otwarcia.
2. Wdrożenie SZBI zgodnego z wymaganiami Ustawy KSC, RODO, NIS2 wraz z politykami i dokumentami tematycznymi oraz innymi odpowiednimi dokumentami w zakresie nie mniejszym niż:
 - a. Opracowanie polityki, procedur szacowania ryzyka wystąpienia incydentu wraz z metodologią dostosowaną do potrzeb i specyfiki oraz narażenia podmiotu zamawiającego. Przeprowadzenie pełnej analizy ryzyka za pomocą opracowanej metodyki, w zakresie nie mniejszym niż: przeprowadzenie analizy ryzyka, ocena ryzyka, opracowanie planu działania, opracowanie rekomendacji wdrażania środków ochrony wraz z oszacowaniem niezbędnych zasobów finansowych oraz ludzkich.
 - b. Opracowanie odpowiednich i proporcjonalnych środków organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyko, skutki społeczne i gospodarcze wystąpienia incydentów. Opracowanie zaleceń dotyczących wdrożenia środków technicznych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie

podmiotu na ryzyka, skutki społeczne i gospodarcze wystąpienia incydentów.

W szczególności:

- i. Opracowanie polityki bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne.
 - ii. Opracowanie odpowiednich dokumentów w zakresie utrzymania i bezpiecznej eksploatacji systemu informacyjnego z uwzględnieniem bezpieczeństwa w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego.
 - iii. Opracowanie dokumentacji bezpieczeństwa fizycznego i środowiskowego, uwzględniające kontrolę dostępu.
 - iv. Opracowanie dokumentacji w zakresie bezpieczeństwa zasobów ludzkich.
 - v. Opracowanie dokumentacji i procesów w zakresie bezpieczeństwa i ciągłości łańcucha dostaw. Opracowanie propozycji zapisów w umowach.
 - vi. Opracowanie, planów działania (zarządzania kryzysowego) umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie i nieoczekiwanych zakłóceniach (tzw. wszechstronna strategia przywracania).
 - vii. Opracowanie zaleceń dotyczących monitoringu w trybie ciągłym w oparciu o analizę ryzyka. Opracowanie listy aktywów, podlegających monitoringowi w trybie ciągłym, biorąc pod uwagę występujące ryzyko oraz koszty wdrożenia i utrzymania.
 - viii. Opracowanie polityk i procedur oceny skuteczności zabezpieczeń technicznych i organizacyjnych.
 - ix. Opracowanie polityk i procedur edukacji z zakresu cyberbezpieczeństwa dla personelu podmiotu w tym zasad cyberhigieny.
 - x. Opracowanie polityki i procedur stosowania kryptografii w tym szyfrowania.
 - xi. Opracowanie polityk i procedur oraz wdrożenie oprogramowania w zakresie zarządzania aktywami.
 - xii. Opracowanie polityki kontroli dostępu.
3. Opracowanie zasad zbierania informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usług wraz z planem wdrożenia działań operacyjnych, obejmującym szacunek zasobów koniecznych do realizacji zadania proporcjonalne do występującego ryzyka.
4. Opracowanie polityki i procedur lub innych koniecznych dokumentów w zakresie zarządzania incydentami, w tym w szczególności:
 - a. Opracowanie zasad stosowania środków zapobiegających i ograniczających wpływ incydentów na funkcjonowanie organizacji zamawiającego.
 - b. Opracowanie zasad stosowania mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym proporcjonalnie do występującego ryzyka.
 - c. Opracowanie zasad dotyczących regularnego prowadzenie aktualizacji oprogramowania, w tym sposobów oceny – wpływu na bezpieczeństwo i poziom krytyczności oraz stosowanie do zaleceń producenta uwzględniając i równoważąc zasady poufności i integralności.
 - d. Opracowanie zasad ochrony przed nieuprawnioną modyfikacją w systemie informacyjnym.



- e. Opracowanie zasad i procedur niezwłocznego podejmowanie działań po dostrzeżeniu podatności.
 - f. Opracowanie zasad i zaleceń oraz wskazanie systemów do stosowania MFA – uwierzytelnianie wieloskładnikowego.
 - g. Opracowanie planu reagowania na incydenty, który określa procedury, odpowiedzialności i kroki do podjęcia w przypadku naruszenia bezpieczeństwa informacji.
5. Opracowana przez wykonawcę dokumentacja bezpieczeństwa systemu informacyjnego będzie stanowić nie mniej niż:
- a. Dokumentację systemu zarządzania bezpieczeństwem informacji;
 - b. Dokumentację ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa, obejmująca:
 - i. charakterystykę usługi oraz infrastruktury, w której świadczona jest usługa,
 - ii. ocenę aktualnego stanu ochrony infrastruktury,
 - iii. szacowanie ryzyka dla obiektów infrastruktury,
 - iv. plan postępowania z ryzykiem,
 - v. opis zabezpieczeń technicznych obiektów infrastruktury,
 - vi. zasady organizacji i wykonywania ochrony fizycznej infrastruktury,
 - vii. dane o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995.), chroniącej infrastrukturę – jeżeli występuje;
 - c. Dokumentacja systemu zarządzania ciągłością działania;
 - d. Dokumentacja techniczna systemu informacyjnego wykorzystywanego do świadczenia usługi;
 - e. Dokumentacja wynikająca ze specyfiki świadczonej usługi w danym sektorze lub podsektorze.
6. Wykonawca określi role i odpowiedzialności, podział zadań i obowiązków w systemie zarządzania bezpieczeństwem informacji i ochrony danych osobowych w ramach integralnego SZBI.
7. W razie wątpliwości dotyczących przygotowanej przez wykonawcę dokumentacji, np. jej zakresu lub interpretacji zapisów mniejszego OPZ, w zakresie wymagań dotyczących wdrożenia systemu zarządzania bezpieczeństwem informacji oraz systemu zarządzania ciągłością działania, zmagający jako punkt odniesienia będzie stosował najnowszy stan wiedzy zawarty w odpowiednich normach europejskich i międzynarodowych, w tym w szczególności w najnowszej wersji Polskiej Normy PN-EN ISO /IEC 27001 - Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności oraz najnowszej wersji Polskiej Normy PN-EN ISO/IEC ISO 22301- Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania. Zamawiający do osiągnięcia ww. celu wykorzysta również Poradnik NASK Cyberbezpieczny samorząd Warszawa 2023 – poradnik dotyczący realizacji projektów z działania 2.2 pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa” do którego wykorzystania jest zobowiązany wymogami realizacji dofinansowanego projektu.
8. Wykonawca przedstawi niezbędne zasoby ludzkie i finansowe niezbędne do wdrożenia i utrzymania opracowanego Systemu Zarządzania Bezpieczeństwem Informacji.
9. Przygotowana przez wykonawcę dokumentacja powinna regulować w szczególności elementy wymienione w załączniku nr.1

Zadanie to będzie realizowane razem z podzadaniem 2.1 w obszarze kompetencyjnym oraz 3.1 w obszarze technicznym.

Zadanie 2 – Obszar kompetencyjny - Szkolenia z cyberbezpieczeństwa.

Szkolenia dla pracowników wraz z kadrą kierowniczą i najwyższym kierownictwem Urzędu Miejskiego w Dąbrowie Górniczej z zagadnień dotyczących cyberbezpieczeństwa.

Tematyka szkoleń dotyczyć będzie świadomości cyberzagrożeń, cyberhigieny, sposobów ochrony oraz aspektów prawnych cyberbezpieczeństwa, w tym w szczególności zaktualizowanego SZBI zamawiającego i wprowadzonych nim procedur oraz działań operacyjnych, zagrożeń bezpieczeństwa informacji, sposobów identyfikacji podejrzanych wiadomości e-mail, bezpiecznego korzystania z haseł, zabezpieczania urządzeń mobilnych, sposobów ochrony danych ze szczególnym uwzględnieniem danych prawnie chronionych oraz danych osobowych.

Przed przeprowadzeniem szkolenia wykonawca uzgodni z zamawiającym program każdego szkolenia.

SZCZEGÓŁOWY ZAKRES SZKOLEŃ

Wszyscy pracownicy

1. Bezpieczeństwo informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań prawnych.
 - Wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa.
 - Wymagania dla pracowników wynikające z przepisów prawa ze szczególnym uwzględnieniem uoKSC oraz RODO.
 - System Zarządzania Bezpieczeństwem Informacji w praktyce.
2. Przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z Internetu.
 - Ochrona informacji i prywatność w Internecie.
 - Bezpieczne korzystanie z poczty elektronicznej.
 - „Inżynieria społeczna” stosowane socjotechniki (ataki psychologiczne) przez cyberprzestępców.
 - Sposoby zabezpieczenia danych i informacji wysyłanych pocztą elektroniczną.
 - Zasady bezpieczeństwa wynikające z użytkowania urządzeń mobilnych (laptopy, tablety, smartfony) i pamięci przenośnych (szyfrowanie).
 - Nieuprawniony dostęp do danych w tym kradzież informacji i danych organizacji od wewnątrz i z zewnątrz,
 - Ransomware jako poważne zagrożenie dla JST.
 - Phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise).
 - Spear phishing, ataki ukierunkowane na konkretne osoby lub organizacje (w tym kadrę kierowniczą)
 - Cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne.
 - Bezpieczne hasła i uwierzytelnienie wieloskładnikowe.
 - Wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa.

Kadra kierownicza

1. Podstawy prawne cyberbezpieczeństwa, ze szczególnym uwzględnieniem obowiązków wynikających z Ustawy KSC.

2. Budowanie kultury cyberbezpieczeństwa w organizacji.
3. Wymogi wynikające z przepisów prawa ze szczególnym uwzględnieniem, uoKSC i RODO
4. Przegląd znanych typów ataków na JST.
5. Podnoszenie świadomości w zakresie szeroko rozumianego bezpieczeństwa teleinformatycznego, ochrony danych osobowych w świetle RODO i bezpieczeństwa informacji w organizacji.
6. Aktualne zagrożenia cybernetyczne dla administracji publicznej.
7. Doskonalenie kompetencji i uczestnictwo kadry kierowniczej w zakresie tworzenia i wdrażania polityk bezpieczeństwa.
8. Przegląd nowoczesnych narzędzi i usług cyberbezpieczeństwa (jako wsparcie procesu zakupowego).
9. Zarządzanie ryzykiem w bezpieczeństwie informacji i obszarach technicznych.
10. System Zarządzania Bezpieczeństwem Informacji – jak skutecznie wdrożyć SZBI.
11. Ciągłość działania – dlaczego jest istotna i jak ją wdrożyć i utrzymywać.
12. Współpraca w ramach s46.
13. Identyfikowanie zagrożeń – jak wdrożyć odpowiednie zabezpieczenia.
14. Współpraca z organami właściwymi w zakresie cyberbezpieczeństwa.
15. Współpraca z Prezesem Ochrony Danych Osobowych w zakresie zgłaszania naruszeń związanych z przetwarzaniem danych osobowych.

Specjaliści IT

1. Podstawy bezpieczeństwa sieci.
2. Aspekty techniczne najpopularniejszych ataków i metody reagowania.
3. Zabezpieczanie poczty elektronicznej.
4. Zabezpieczanie serwisów www.
5. Ochrona przed atakami DDoS.
6. Profilaktyka cyberzagrożeń ze szczególnym uwzględnieniem zarządzania kopiami zapasowymi.
7. Przegląd źródeł wiedzy o zagrożeniach.
8. Podstawy zabezpieczenia ciągłości działania.
9. Identyfikacja podatności i aktualizacja oprogramowania.
10. Zarządzanie incydemem.

W ramach tego zadania planowane jest przeprowadzenie w trakcie trwania projektu nie mniej niż 3 szkoleń dla pracowników Urzędu. Łącznie cyklem szkoleń zostanie objętych nie mniej niż 440 osób, a nie więcej niż 500 osób. Każde szkolenie będzie organizowane w ilości terminów niezbędnych do przeszkolenia co najmniej 440 pracowników.

Szkolenia będą realizowane stacjonarne w siedzibie Urzędu miejskiego w Dąbrowie Górniczej przy ul. Granicznej 21. Harmonogram szkoleń zostanie uzgodniony i zatwierdzony przez zamawiającego.

Szkolenia zostaną rozłożone równomiernie w harmonogramie realizacji projektu tj.

- na początku projektu w zakresie uświadomienia wyzwań oraz wymagań prawnych z obszaru cyberbezpieczeństwa,
- w późniejszym okresie po realizacji zadania przeglądu i aktualizacji dokumentacji SZBI, z zakresu stosowania zaktualizowanego SZBI,
- w końcowej fazie projektu w celu wdrożenia produktów Zadania 3 - System wspomagający proces analizy ryzyka oraz zarządzania incydentami.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Szkolenia będą dostosowane dla grup odbiorców: pracownicy, kadra zarządzająca, najwyższe kierownictwo. Za zgodą Zamawiającego część szkoleń może odbyć się w sposób zdalny.

Szkolenia przeprowadzone w ramach zadania 2 zostaną wprowadzone do platformy eLearningowej stanowiącej jedną z funkcjonalności oprogramowania zamawianego w Zadaniu 3.

Wykonawca zapewni utrzymywanie aktualności szkoleń w ramach wdrożonej platformy przez okres trwania umowy.

Zadanie 3 - Obszar techniczny - System wspomagający proces analizy ryzyka oraz zarządzania incydentami.

Wykonawca wdroży system informatyczny wspomagający procesy zarządzania incydentami bezpieczeństwa i ochroną danych osobowych oraz analizy ryzyka usprawniającego realizację zadań w ramach wdrożonych procedur zarządzania bezpieczeństwem informacji z zadania 1, przyczyniając się jednocześnie do realizacji kluczowych celów dyrektywy NIS2, ustawy KSC oraz stosowania przepisów RODO.

W chwili obecnej urząd nie posiada systemu informatycznego wspierającego i monitorującego poprawne funkcjonowanie procedur SZBI.

Dzięki wdrożeniu systemu ma zostać zapewnione wsparcie realizacji wymaganych przepisami prawa procesów z zakresu bezpieczeństwa informacji oraz zarządzania procesami w szczególności.:

- upoważnieniami dopuszczającymi (nadawanie, zarządzanie zmianą, odbieranie uprawnień),
- incydentami i zgłoszeniami naruszeń bezpieczeństwa i ochrony danych osobowych,
- analiza ryzyka w bezpieczeństwie informacji i ochrony danych osobowych,
- zbieranie dowodów na zgodność z procedurami,
- wspomaganie szkoleń w systemie e-learningowym,
- prowadzeniem rejestrów wymaganych przepisami prawa.

System ma być dostępny dla min. 500 użytkowników końcowych w modelu subskrypcyjnym.

System ma zapewnić funkcjonalności w zakresie nie mniejszym niż:

- zdefiniowania własnej skali ryzyka i jej późniejszej modyfikacji przez administratora,
- przeprowadzenia analiz ryzyka dla elementów pochodzących ze stworzonych słowników oraz tych utworzonych przez zamawiającego,
- uwzględniania w analizie zmodyfikowanych wartości z utworzonych słowników, definiowania własnych reguł obliczeń dla pól formularzy, definiowania własnych arkuszy analizy ryzyka,
- realizacji wszystkich rodzajów analiz określonych w przepisach dot. ochrony danych osobowych, m. in.: analizy ryzyka, oceny ryzyka naruszenia, testów równowagi, oceny skutków przetwarzania,
- realizacji analiz ryzyka naruszeń i incydentów dot. cyberbezpieczeństwa,
- zdalnego audytu podmiotów przetwarzających,
- prowadzenia dowolnych rejestrów dot. zarządzania bezpieczeństwem informacji w tym w szczególności rejestrów dot. Systemów IT, w tym: rejestr zasobów IT, typy zasobów IT, rejestrów zniszczenia/usunięcia danych i nośników, rejestry uprawnień, rejestry kopii zapasowych itp.,
- klasyfikacji informacji oraz zarządzania aktywami,
- definiowania i generowania dowolnych raportów w formatach: *.docx, *.xlsx z automatycznym wypełnieniem pól na podstawie tagów referujących do pól formularza,
- sugestii podczas przeprowadzania analizy, np. poprzez proponowanie odpowiednich zagrożeń na podstawie ustalonej listy podatności,
- dokumentowania realizowanych audytów,
- automatycznej analizy udzielanych odpowiedzi w ankietach oraz opracowana protokołu identyfikującego kluczowe obszary ryzyka,

- korzystania z funkcjonalności bazy wiedzy, która automatycznie wspiera w wypełnianiu formularzy związanych z cyberbezpieczeństwem i RODO np. w opisie zasobów, analizie ryzyka. Przykład: na podstawie opisu charakteru przetwarzania, aplikacja będzie miała funkcjonalność proponowania potencjalnego ryzyka, zagrożenia i podatności,
- logowania MFA - z wykorzystaniem tokenów autoryzacyjnych Google/Microsoft Authenticator,
- zarządzania uprawnieniami opartymi na rolach, w tym możliwość tworzenia grup lokalnych, definicja uprawnień dla właścicieli grupy,
- definiowania i dziedziczenia uprawnień,
- pełnej konfiguracji słowników, w tym zmiany schematu struktury słowników przez Klienta,
- zarządzania słownikami, w tym nielimitowanego dodawania nowych rozwiązań bez koniecznej ingerencji w kod źródłowy aplikacji,
- zarządzania workflow i procesami, w tym tworzenia nowych i modyfikacja procesów dotyczących wprowadzania informacji do formularzy przez określonych pracowników, na poszczególnych etapach procesów,
- definiowania czasowych dostępów dla użytkowników do zasobów, w tym np. możliwość zmiany przypisania licencji do innych użytkowników w trakcie trwania umowy – w ramach dostępnej puli,
- możliwość wykorzystania podpisu wewnętrznego,
- definiowania procesów składających się z dowolnej ilości akcji, których kolejność warunkowana jest wynikiem walidacji formularzy na podstawie zdefiniowanych warunków,
- wysyłania powiadomień o zmianie statusu dla danego procesu, w kontekście danego rekordu,
- definiowania ścieżki realizacji zadań, które będą automatycznie uruchomione po wystąpieniu określonych warunków,
- generowania dokumentów na podstawie szablonów,
- generowania umów powierzenia na podstawie zdefiniowanych szablonów *.docx,
- definiowania filtrów i ich zapisania do przeszukiwania rekordów wg zawartości,
- zmiany nazwy dla elementów menu wg wymagań Zamawiającego,
- tworzenia obiegów dot. nadawania lub zmiany uprawnień i upoważnień,
- importu i danych z dowolnego pliku *.xlsx bez konieczności dostosowania do zadanego szablonu importu, na podstawie przyporządkowania w trakcie importu kolumn z pliku do zawartości słowników,
- exportu wszystkich danych merytorycznych wraz z powiązaniem w postaci plików co najmniej w *.xlsx

System musi zapewniać:

- dokumentację w formie elektronicznej z samouczkami w języku polskim,
- dostępność z powszechnie stosowanych przeglądarek internetowych z możliwością dostępu do wszystkich funkcjonalności na tabletach i smartfonach z Android/iOS/Windows, w tym w szczególności Edge i Firefox,
- aktualizację w okresie dostępu do systemu do najnowszej wersji w tym w szczególności dostosowujący system do zmieniających się przepisów prawa i wymagań bezpieczeństwa.

Wymagania dodatkowe, zamawiający oczekuje:

- możliwości logowania się do systemu bez konieczności instalowania jakichkolwiek dodatkowych komponentów oprócz z przeglądarki internetowej w aktualnej stabilnej wersji,

- utrzymania systemu w formule oprogramowanie jako usługa tj. zapewnienie architektury i ciągłości działania usługi bez konieczności zapewnienia hostingu przez Zamawiającego.

Wymagania wobec Wykonawcy:

- Dostarczyć w pełni funkcjonujące oprogramowanie. Oprogramowanie ma zawierać wszystkie funkcjonalności gotowe do użycia,
- Zapewnienie i realizacja wsparcia do oprogramowania.
- Aktualizację systemu wg aktualnych wytycznych, jego dostosowanie i implementacja zmian wynikających z wymagań prawa;
- Przegląd systemu i logów, celem podnoszenia jakości i wdrażania uwag użytkowników tzw. User experience;
- Wykonywanie kopii zapasowej systemu oraz danych i udostępnianie ich na życzenie zamawiającego w terminie do 3 dni roboczych. Odtworzenie kopii zapasowej na życzenie zamawiającego ma nastąpić w ciągu 12 godzin roboczych,
- Zapewnienie obsługi gwarancyjnej;
- Przeprowadzanie okresowych szkoleń z nowych funkcjonalności i aktualizację dokumentacji wchodzącej w skład instrukcji, w tym samouczków;
- Jeżeli oferowane oprogramowanie opiera się lub wykorzystuje technologię firm trzecich to komponenty te, dla Zamawiającego muszą być legalne i na bieżąco aktualizowane oraz zgodne z polityką licencjonowania firmy trzeciej. Powinna zawierać na bieżąco pojawiające się poprawki bezpieczeństwa,
- Jeżeli oferowane oprogramowanie opiera się o komponenty wymagające odpłatnego licencjonowania ze strony Zamawiającego to koszty z tym związane muszą być sfinansowane przez dostawcę usługi, a licencje przekazane Zamawiającemu.
- Zapewnienie kompatybilności Oprogramowania z najnowszą wersją każdego z komponentów programowych niezbędnych do prawidłowego ich działania oraz z najnowszą wersją przeglądarki internetowej. W przypadku wykrycia braku wyżej określonej kompatybilności Wykonawca niezwłocznie dostarczy wersję kompatybilną, jednak nie później niż w terminie nie dłuższym niż 30 dni od czasu wykrycia i zgłoszenia przez Zamawiającego lub pozyskania przez Wykonawcę informacji o ww. niekompatybilności za pomocą ogólnodostępnych źródeł informacji. Za zgodą Zamawiającego termin 30 dni może ulec wydłużeniu w przypadku, jeśli niekompatybilność ta nie wpływa rażąco na funkcjonalność Oprogramowania lub nowsza wersja komponentu, który stracił kompatybilność nie jest konieczna z punktu widzenia bezpieczeństwa systemów Zamawiającego.
- Utrzymania bezpieczeństwa oprogramowania i przetwarzanych za jego pomocą danych w pełnym zakresie.
- Regularnego przeprowadzania testów bezpieczeństwa Oprogramowania prowadzonego przez zewnętrzne podmioty specjalizujące się w zagadnieniach cyberbezpieczeństwa. Przedstawianie na życzenie zamawiającego wyników testów potwierdzających odpowiedni poziom bezpieczeństwa oprogramowania.
- Zapewnienia w sposób ciągły usuwania wad Oprogramowania wpływających na obniżenie bezpieczeństwa informacji.
- Zamawiający zastrzega sobie możliwość przeprowadzania testów bezpieczeństwa Oprogramowania. Wykonawca jest zobowiązany do usunięcia wykrytych wad Oprogramowania do 30 dni od czasu powiadomienia przez Zamawiającego.

- Bieżącego przekazywania informacji mogących mieć wpływ na cyberbezpieczeństwo Oprogramowania i wszystkich elementów konfiguracji środowiska, w którym działa Oprogramowanie.
- Wykorzystywanie nowoczesnych rozwijanych technologii w celu podnoszenia bezpieczeństwa Oprogramowania.
- Zapewnienie prawidłowej konfiguracji i odpowiedniego poziomu zabezpieczeń dla modułów udostępnionych w sieci Internet.

Obsługa awarii

AWARIA – to niepoprawne działanie oprogramowania, udostępnionego Zamawiającemu przez Wykonawcę, które prowadzi do całkowitego zatrzymania eksploatacji oprogramowania, jak również niepoprawne, powtarzalne i niezgodne z dokumentacją działanie kluczowych funkcji dostępnych w oprogramowaniu dotyczące każdego użytkownika i każdego środowiska pracy oprogramowania spełniającego minimalne wymagania producenta, które nie może być zastąpione przez Zamawiającego alternatywną metodą pracy lub Wykonawca nie jest w stanie zaproponować alternatywnej metody pracy, w efekcie doprowadzając do braku możliwości wykorzystania funkcji zakupionego oprogramowania.

W zakresie obsługi awarii Zamawiający oczekuje:

- udzielania konsultacji telefonicznych w dni robocze w godzinach 8.00 – 16.00 przez chat oraz pod wskazanym numerem telefonu.
- udzielania konsultacji zdalnych za pomocą systemu pomocy TeamViewer (wgląd w system zamawiającego).
- czasy obsługi:
 - czas reakcji na zgłoszoną awarię – do 4 godzin roboczych,
 - czas usunięcia awarii lub zapewnienie alternatywnego sposobu pracy na Systemie – do 40 godzin roboczych,

Podane terminy mogą ulec zmianie, każdorazowo w wyniku ustaleń pomiędzy stronami, jak i w przypadku, kiedy usuwanie powyższych problemów jest niemożliwe z powodów, na które Wykonawca nie miał bezpośredniego wpływu. Termin może ulec zmianie jedynie w przypadku wniosku o przedłużenie złożonego przed terminem jego realizacji.

Za godziny robocze uznaje się czas od poniedziałku do piątku w godzinach pomiędzy 8.00 a 16.00 z wyłączeniem dni ustawowo wolnych od pracy;

- analizy, wskazania przyczyny i usunięcia nieprawidłowego działania systemu objętego umową,
- wyznaczenie jednego punktu kontaktu - systemu internetowych zgłoszeń elektronicznych dostępnych na stronie Wykonawcy (adres strony www systemu zgłoszeń) służącego do zgłaszania awarii. Każde zgłoszenie w tym systemie powinno zostać zarejestrowane, uzyskać numer ewidencyjny oraz zawierać datę i godzinę przyjęcia. System przyjmowania zgłoszeń Wykonawcy powinien automatycznie bezzwłocznie potwierdzić drogą e-mail fakt otrzymanie zgłoszenia oraz terminu jego realizacji. W przypadku awarii systemu zgłoszeń Wykonawcy Zamawiający prześle zgłoszenie na wskazaną w umowie skrzynkę poczty elektronicznej wykonawcy wraz z potwierdzeniem dostarczenia wiadomości e-mail i czas zgłoszenia będzie się liczył od momentu wygenerowania automatycznego zgłoszenia z serwera poczty e-mail Zamawiającego.
- Zapewnienie prowadzenia możliwości konsultacji oraz wsparcia eksperta w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa, możliwość zadawania pytań dla 5 osób

z organizacji zamawiającego w okresie trwania umowy, w szczególności zadawania pytań dotyczących przygotowanego SZBI oraz jego ewentualnych zmian lub potrzeby doskonalenia wynikającego z praktyki jego stosowania w organizacji lub zmieniającego się otoczenia technologicznego lub prawnego. Doradztwa z zakresie dostosowania aplikacji do potrzeb zamawiającego w zakresie jej funkcjonalności.

Dostarczona przez wykonawcę w systemie funkcjonalność platformy eLearningowej zapewni:

- możliwość samodzielnego tworzenia szkoleń przez zamawiającego m.in. możliwość korzystania z kreatora slajdów ze wstępnie skonfigurowanymi slajdami szkoleniowymi,
- możliwość potwierdzania odbycia szkoleń i instruktaży poprzez zaświadczenia i certyfikaty, które można samodzielnie dodawać i edytować,
- utrzymanie aktualności przygotowanych przez wykonawcę szkoleń w okresie trwania umowy,
- możliwość samodzielnej konfiguracji przez zamawiającego procesów zatrudnienia z wymaganymi szkoleniami i egzaminami tak by pracownik mógł odbyć szkolenie, zapoznać się z dokumentem, złożyć epodpis, zdać egzamin, otrzymać certyfikat i upoważnienie do przetwarzania (automatycznie) tak by całość procesu została w znaczący sposób zautomatyzowana i oparta na gotowych szablonach i kolejnych uprzednio zdefiniowanych następujących po sobie etapach,
- możliwość dodawania własnych egzaminów ze skonfigurowaną punktacją np. pytania wielokrotnego wyboru z punktami ujemnymi,
- możliwość ustawienia ułatwień dla osób słabosłyszących, w tym powiększenie, zmiana kolorystyki,
- możliwość ustawienia ułatwień dla osób słabowidzących, w tym transkrypcja audio. Aplikacja dostarczona przez wykonawcę ma spełniać wymagania prawne w zakresie dostępności cyfrowej.

załącznik nr 1

Przygotowana przez wykonawcę dokumentacja powinna zawierać w szczególności :

DOKUMENTACJA O CHARAKTERZE OGÓLNYM

- deklaracje Administratora danych osobowych o wdrożeniu SZBI oraz zarządzenia / polecenie,
- zasady określające prawa i wolności – tj. realizację praw osób, których dane dotyczą - Opis zasad realizacji praw osób, których dane dotyczą (Art. 7 ust. 3, Art. 12 – 22),
- zasady określające politykę prywatności i politykę cookies na stronach internetowych Urzędu,
- zasady określające korzystanie z urządzeń (m.in. zastosowanych w organizacji mechanizmów zabezpieczających związanych z wykorzystywaniem urządzeń mobilnych),
- zasady określające pracę zdalną,
- zasady określające audyty wewnętrzne (metodyka, procedury, wyszkolenie zespołu, przeglądy i zarządzanie wnioskami z audytu).

ZASADY DOTYCZĄCE OCHRONY INFORMACJI

- zasady bezpiecznego przetwarzania informacji i danych osobowych przez pracowników,
- określenie i uregulowanie następujących zasad: czystego biurka, czystego ekranu, czystego wydruku, czystego kosza, zasada kontroli nad kopiami dokumentów, poufności rozmów, nadzorowania petentów, prywatności kont w systemach, poufności haseł i kodów dostępu, korzystania z Internetu, korzystania z oprogramowania oraz zamkniętego pomieszczenia, polityka zabezpieczenia kluczy oraz haseł do pomieszczeń), minimalnego (najmniejszego) uprzywilejowania (ang. principle of least privilege) w zakresie nadawanych uprawnień dla użytkowników oraz uprawnień administracyjnych,
- zasady wykorzystania rozwiązań chmurowych,
- zasady zarządzania dostępem do usług informatycznych, w tym katalog usług cyfrowych urzędu,
- zasady zarządzania mechanizmami uwierzytelniającymi, w tym hasłami (polityka haseł i dostępu),
- zasady publikacji informacji (zwłaszcza wizerunku osób) na stronach Urzędu Miejskiego (w tym wszystkie nasze www, BIP, Facebook itd.),
- zasady bezpieczeństwa informacji w kontekście rozliczalności wszystkich użytkowników ze szczególnym uwzględnieniem działań administratorów,
- zasady wewnętrznej wymiany danych (dyski i foldery sieciowe, porty USB, rozwiązania chmurowe),
- zasady wykorzystywania zabezpieczeń biometrycznych,
- zasady zarządzania mechanizmami kryptograficznymi – szyfrowanie danych osobowych,
- zasady monitorowania przepisów prawnych związanych z zabezpieczeniem przetwarzanych informacji i danych osobowych oraz wprowadzania zmian wynikających z obowiązków prawnych,
- zasady postępowania z nośnikami informacji, w tym składowanie i wymiana nośników oraz niszczenie informacji zapisanych na nośnikach,
- zasady dotyczące założenia i prowadzenie rejestru haseł,



- zasady nagrywania rozmów telefonicznych,
- zasady bezpiecznego korzystania z urządzeń mobilnych (telefony, sprzęt: laptop, tablet itd.),
- zasady i wytyczne dostępu do systemu centralnego wydruku oraz zabezpieczenia wytworzonych na nim dokumentów,
- zasady zabezpieczania danych podczas wymiany informacji i danych osobowych z podmiotami zewnętrznymi,
- zasady konsultacji z IOD dotyczące przetwarzania danych osobowych przez komórki Urzędu,
- zasady privacy by design i privacy by default – dokument powinien określać w jaki sposób zapewnić odpowiedni poziom bezpieczeństwa danych i prawa do prywatności (Art. 25 RODO),

UMOWY POWIERZENIA - WSPÓŁPRACA Z PODMIOTAMI ZEWNĘTRZNYMI

- zasady wymiany danych z podmiotami zewnętrznymi (umowy powierzenia, umowy serwisowe, umowy główne, ankieta bezpieczeństwa wraz z oświadczeniem wypełniającego audyty zewnętrzne, regularne monitorowanie i sprawdzanie zgodności działań stron trzecich z umową oraz przepisami dotyczącymi ochrony danych i cyberbezpieczeństwa),
- zasady kontroli podmiotów przetwarzających - opisanie zasad kontroli procesorów (podwykonawców) – (Art. 28 ust. 3 lit. h) RODO), (referencje, certyfikaty bezpieczeństwa, audyty zewnętrznych),
- zasady bezpieczeństwa informacji i ochrony danych osobowych w relacjach z dostawcami – opracowanie procesów i ich wdrożenie zarządzania ryzykami związanych z użyciem produktów lub usług w relacji z dostawcami zewnętrznymi (w tym ryzyka związane z łańcuchem dostaw produktów i usług informacyjno-telekomunikacyjnych),
- zasady dotyczące monitorowania, przeglądu, oceny, zmiany praktyk w zakresie bezpieczeństwa informacji.

REGULACJE DOTYCZĄCE OPROGRAMOWANIA

- zasady zakupu, wdrażania, eksploatacji i wycofywania oprogramowania,
- zasady zarządzania kopiami zapasowymi/archiwalnymi,
- zasady aktualizacji oprogramowania,
- zasady zarządzania podatnościami,
- zasady zarządzania inwentaryzacją sprzętu i oprogramowania.

RETENCJA DANYCH

- zasady retencji danych w tym w szczególności zasady retencji danych poczty służbowej i innych niezbędnych wskazanych przez wykonawcę.

OPRACOWANIE

- zasad prowadzenia rejestrów czynności przetwarzania w komórkach organizacyjnych Urzędu - opis wszystkich procesów przetwarzania danych osobowych zachodzących w organizacji wraz ze wzorem rejestru,

- zasad w zakresie utrzymywanie komunikacji pomiędzy wszystkimi działami i działem zarządzania zasobami ludzkimi oraz z przełożonymi osób zaangażowanych w przetwarzanie informacji (relacje IOD - KADRY - WYDZIAŁ)
- zasad inwentaryzacji zasobów (aktywów) związanych z przetwarzaniem informacji (sprzęt informatyczny, serwery i infrastruktura sieciowa, zasoby ludzkie, usługi w chmurze, informacje powierzone przez klientów, pomieszczenia i lokalizacje, z ustaleniem właściciela poszczególnych zasobów i niezbędne inne wskazane przez wykonawcę),
- zasad w zakresie zapewnienia zasilania awaryjnego,
- zasad dla pracowników dotyczące działania po awarii, ich zgłaszania, z przywracania działania systemu, ograniczania potencjalnych szkód,
- zasad zachowania i reagowania na incydenty cyberbezpieczeństwa.
- zasady ograniczania uprawnień administracyjnych.

SZKOLENIA I BEZPIECZEŃSTWO OSOBOWE

- stworzenie i wdrożenie zasad weryfikacji i nadzoru, który zapewni, że osoby zaangażowane w proces przetwarzania informacji będą do tego uprawnione oraz że będą się angażować w sposób odpowiedni do swoich zadań,
- opracowanie zasad szkoleń z zakresu ochrony danych osobowych i informacji oraz cyberbezpieczeństwa tj. dokument opisujący i określający zasady prowadzenia szkoleń dla personelu uczestniczącego w przetwarzaniu danych osobowych i informacji (instruktaże i szkolenia wstępne, doskonalące, okresowe itd. – kto, kiedy, jak i gdzie) – (Art. 39 RODO),
- wzór materiałów informacyjnych dla pracowników (kompendium ochrony danych osobowych) – podnoszenie świadomości pracowników w zakresie ochrony danych osobowych (Art. 39 RODO),
- zasady zarządzania dostępem do informacji, w tym nadawania, modyfikacji, odbierania uprawnień oraz przeglądu uprawnień,
- zasady regularnego aktualizowania uprawnień i weryfikacji osób zaangażowanych w proces przetwarzania danych (proces zarządzania zmianą),
- opracowanie zasad dotyczących zabezpieczenia osobowego podczas zatrudnienia (m.in. w przypadku naruszenia PBI, po ustaniu zatrudnienia, oświadczenia o poufności lub nie ujawnianiu informacji, określenie przypadków pracy zdalnej poza siedzibą Urzędu, opracowanie mechanizmu niezwłocznego powiadomienia o zdarzeniach za pośrednictwem odpowiednich kanałów) itd.,
- zasady związane z odejściem pracownika oraz zablokowanie poczty (opcją informowania nadawców, że skrzynka została zablokowana) połączone z obowiązkiem czyszczenia przez właściciela konta wiadomości zwłaszcza prywatnych oraz przerzucenia istotnych informacji firmowych na zasób komórki,
- zasady ustalenia odpowiednich zabezpieczeń dostępu do informacji, takich jak hasła, identyfikatory, autoryzacja dwuetapowa itp. tak by upewnić się, że wyłącznie upoważnione osoby mają dostęp do informacji,
- zasady w zakresie logowania działań użytkowników i monitorowania dzienników zdarzeń systemowych.

WZORY DOKUMENTÓW

- wzory klauzul informacyjnych RODO (art. 13 i 14 RODO),

- wzory zgód na przetwarzanie danych osobowych,
- wzór rejestrów czynności przetwarzania i rejestr kategorii czynności przetwarzania dla komórek organizacyjnych,
- wzór rejestru kategorii czynności przetwarzania w komórkach organizacyjnych – czyli rejestr wszystkich informacji w zakresie danych, które zostały organizacji powierzone (Art. 30 ust. 2 RODO) + wzór rejestru,
- wzór raportu z ocen skutków dla ochrony danych osobowych.

NARUSZENIA

- zasady zgłaszania naruszeń do organu nadzorczego PUODO zgodnie z RODO (Art. 33 RODO),
- rejestr naruszeń ochrony danych osobowych zgodnie z RODO,
- ankieta wspomagająca analizę wystąpienia ryzyka naruszenia praw lub wolności w związku z incydentem ochrony danych osobowych,
- zasady postępowania w przypadku incydentu naruszenia bezpieczeństwa informacji i danych osobowych,
- zasady na wypadek wystąpienia naruszeń - opis postępowania na wypadek wystąpienia naruszeń mogących powodować wysokie ryzyko naruszenia praw i wolności osób, w zakresie ich informowania o działaniach jakie powinni wykonać, aby ryzyko to ograniczyć (Art. 34 RODO).
- zasady zgłaszania naruszeń cyberbezpieczeństwa zgodnie z ustawą KSC (UoKSC).

Harmonogram płatności

Umowa zostanie zawarta na okres 14 miesięcy. Koniec projektu 30.06.2026r.

1. Płatność 1 - Raport z przeglądu dokumentacji SZBI 10%
2. Płatność 2 - Wykonanie szkoleń wstępnych 10%
3. Płatność 3 - Wykonanie aktualizacji dokumentacji SZBI 20%
4. Płatność 4 - Wykonanie szkoleń z zaktualizowanego SZBI 20%
5. Płatność 5 - Wdrożenie programu i przeszkolenie użytkowników 40%.

Kryteria wymagań w stosunku do wykonawcy

Zdolność techniczna lub zawodowa zespołu wdrażającego SZBI:

Do zapewnienia wsparcia merytorycznego na etapie realizacji umowy, zostanie skierowanych minimum 2 specjalistów, z czego co najmniej jeden z nich ma udokumentowane:

1. 10 letnie doświadczenie w audycie bezpieczeństwa informacji;
2. doświadczenie jako inspektor ochrony danych osobowych min. 3 lata;
3. posiadanie uprawnień Auditora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001 – wymagany aktualnego certyfikat, ważny na dzień składania ofert.

Zdolność techniczna lub zawodowa w zakresie szkoleń



Doświadczenie: Wykonawca musi udokumentować zrealizowanie w ciągu ostatnich 3 lat, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych usług w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, że wykonał należycie co najmniej dwie usługi polegające na przygotowaniu i przeprowadzeniu szkoleń z zakresu systemów zarządzania bezpieczeństwem informacji oraz cyberbezpieczeństwa – udokumentowane referencjami o wartości minimum 20 000 zł brutto.

Zdolność techniczna lub zawodowa Oprogramowanie – wymagane doświadczenie

Wykonawca musi udokumentować zrealizowanie w ciągu ostatnich 3 lat, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych usług w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, że wykonał należycie co najmniej dwa projekty w podmiotach zatrudniających min. 200 pracowników polegające na opracowaniu, wdrożeniu i utrzymaniu systemów informatycznych do wsparcia procesu analizy ryzyka oraz zarządzania incydentami w obszarze RODO i cyberbezpieczeństwa – udokumentowane referencjami.

Kary

Wykonawca za odstąpienie od umowy, niewykonanie lub nienależyte wykonanie zapisów umowy przewiduje zastosowanie kar powszechnie stosowanych dla zamówień tego typu.