OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest kompleksowe wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z normą ISO IEC 27001 oraz dyrektywą NIS2.

Zamawiający wymaga wykonania usługi zgodnie z wymaganiami bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych z uwzględnieniem specyfiki uczelni publicznej oraz aktualnie obowiązujących norm PN-EN ISO 27001, PN-EN ISO 27005, PN-EN ISO 22301, a także dyrektywą NIS2 zwanych dalej Normą.

Wdrożenie ma na celu zwiększenie poziomu ochrony informacji oraz zapewnienie ciągłości działania w jednostce poprzez kompleksowe opracowanie, wdrożenie, przegląd i aktualizację dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Na wdrożenie składają się prace audytowe, szkoleniowe, konsultacyjne, wdrożeniowe, weryfikacyjne oraz działania polegające na opracowaniu niezbędnej dokumentacji. Na żądanie Zamawiającego, prace te będą wykonywane bezpośrednio w siedzibie Zamawiającego. Rezultat ma być w pełni zgodny z wymogami krajowymi (w tym ustawy o krajowym systemie cyberbezpieczeństwa – uoKSC, Krajowych Ram Interoperacyjności – KRI) oraz z uznanymi standardami międzynarodowymi (ISO 27001, ISO 27005, ISO 22301, NIS2).

Cel, przedmiot i zakres zamówienia:

Wymagane, aby Wykonawca spełnił poniższe wymagania minimalne:

1. Wykonanie audytu początkowego w celu oceny pierwotnego stanu rzeczy i identyfikacji zagrożeń obejmującego:
    a) Przygotowanie harmonogramu prac składających się z następujących etapów:
        - Etap analityczny (przegląd istniejących dokumentów, ocena ryzyka) powinien zostać wykonany w terminie 12 tygodni od podpisania umowy,
        - Etap opracowania dokumentacji wraz z konsultacjami z Zamawiającym – do 12 tygodni po zakończeniu analizy,
        - Etap wdrożenia i instruktażu – do 12 tygodni po akceptacji dokumentacji,
        - Etap testów, przeglądu i aktualizacji – przeprowadzony w ciągu 12 tygodni od zakończenia wdrożenia (z możliwością powtarzania cyklu w ramach gwarancji).
    b) spełnienia wymagań Normy, w tym wskazanie zakresów wymagających nadzoru (np. infrastruktury IT, wyposażenia, dokumentacji),
    c) inwentaryzacji i kategoryzacji aktywów informatycznych Zamawiającego,
    d) legalności wykorzystywanego oprogramowania,

e) wykonania zewnętrznych testów penetracyjnych infrastruktury IT: analiza topologii sieci na granicy z Internetem, ocena mechanizmów ochronnych, wykrywanie publicznie dostępnych usług sieciowych, identyfikacja wersji i typów publicznie dostępnego oprogramowania, zalecenia dotyczące wzmocnienia ochrony sieci brzegowej,

f) wykonania wewnętrznych testów penetracyjnych infrastruktury IT: ocena struktury sieci LAN, testowanie wewnętrznych zabezpieczeń sieciowych, analiza i monitoring ruchu sieciowego, skanowanie portów i usług w sieci LAN, wykrywanie aktywnych urządzeń w sieci, ocena procedur tworzenia i odzyskiwania kopii zapasowych, rekomendacje dla poprawy bezpieczeństwa wewnętrznej sieci LAN,

g) wykonania audytu bezpieczeństwa serwisów pocztowych: analiza mechanizmów SPF, DKIM i DMARC, ocena zabezpieczeń TLS w komunikacji poczty elektronicznej

h) wykonania audytu bezpieczeństwa serwisów WWW: weryfikacja aktualności serwerów HTTP oraz systemu CMS, ocena bezpieczeństwa komunikacji internetowej,

i) ocenę zgodności z dobrymi praktykami branżowymi oraz przepisami prawa w zakresie bezpieczeństwa i przetwarzania informacji z uwzględnieniem przepisów dotyczących szkolnictwa wyższego dotyczących: RODO, urządzeń i systemów administrowanych przez Centrum informatyczne, a także usług chmurowych,

j) określenie w porozumieniu z Zamawiającym zakresu działań, które muszą być podjęte celem uzyskania zgodności z wymaganiami Normy poprzez przygotowanie planu i harmonogramu prac wdrożeniowych,

k) Określenie zakresu i harmonogramu prac wdrożeniowych.

Zamawiający wymaga, aby audyty zostały przeprowadzone w zgodzie z Krajowymi Ramami Interoperacyjności (KRI) z uwzględnieniem elementów ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) w kontekście Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Zamawiający wymaga, aby na zespole audytorskim spoczywał obowiązek weryfikacji zgodności z innymi przepisami, w tym zgodność z przepisami dotyczącymi ochrony danych osobowych (np. RODO), w kontekście zarządzania danymi, bezpieczeństwa informacji oraz cyberbezpieczeństwa, a także sprawdzenie zgodności z krajowymi i międzynarodowymi normami oraz standardami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem.

2. Opracowanie dokumentacji w zakresie wymaganym przez Normy, dopasowanej do Uczelni, dotyczącej faktycznie obsługiwanych procesów i zintegrowanej z istniejącą dokumentacją. Wykonawca przygotuje szczegółowe dokumenty i zaktualizuje istniejące, regulujące procesy związane z bezpieczeństwem informacji. Muszą one uwzględniać m.in. procedury obsługi incydentów, zasady kontroli dostępu, zarządzanie ryzykiem, bezpieczeństwo pracy zdalnej, wykorzystanie urządzeń mobilnych, szyfrowanie danych, a także planowanie i utrzymanie ciągłości działania. Przedmiotem jest opracowanie i wdrożenie polityk, procedur, planów i instrukcji obejmujących obszary:

    a) Polityka Bezpieczeństwa Informacji (PBI), w tym dokumenty:

        - Procedura czystego biurka i czystego ekranu obejmująca zasady utrzymywania porządku na stanowiskach pracy, tak aby poufne dane (zarówno w formie papierowej, jak i elektronicznej) nie były narażone na wgląd osób nieuprawnionych,

- Procedura klasyfikacji informacji definiująca kategorie ochrony informacji (np. jawne, poufne, wrażliwe), kryteria ich przydzielania oraz sposoby znakowania i przechowywania. Celem jest jasne określenie, jakie poziomy ochrony stosuje się do różnego typu danych, co pozwala zapobiegać niekontrolowanemu ujawnieniu treści o istotnym znaczeniu,
- Procedura bezpieczeństwa zasobów ludzkich zawierająca wytyczne dotyczące rekrutacji, szkolenia oraz wyrejestrowywania pracowników z systemów IT, reguluje zasady podpisywania oświadczeń o zachowaniu poufności, monitorowanie przestrzegania polityk bezpieczeństwa przez personel oraz tryb postępowania w przypadku naruszeń lub odejścia pracownika,
- Procedura zarządzania relacjami z dostawcami obejmująca cały cykl zarządzania podmiotami zewnętrznymi, które otrzymują dostęp do informacji bądź systemów urzędu (np. dostawcy usług IT). Dokument określający m.in. zasady umów powierzenia, ocenę bezpieczeństwa dostawcy, audyty zgodności, mechanizmy weryfikacji,
- Plan szkoleń i podnoszenia świadomości zawierający szczegółowe omówienie sposobów oraz częstotliwości prowadzenia szkoleń dotyczących ochrony informacji,
- Procedura przeprowadzania audytów wewnętrznych określający zasady cyklicznych kontroli wewnętrznych oceniających zgodność z politykami bezpieczeństwa, przepisami (Krajowe Ramy Interoperacyjności, ustawie o Krajowym Systemie Cyberbezpieczeństwa) i normami (ISO 27001). Procedura ta określa zakres, harmonogram, odpowiedzialność, sposób raportowania i analizowania wyników audytów w celu wykrycia ewentualnych niezgodności,
- Procedura działań doskonalących definiujący proces ciągłego doskonalenia SZBI. Po zidentyfikowaniu problemów wyjaśnia, jak zaplanować, przeprowadzić i weryfikować skuteczność działań korygujących i zapobiegawczych,
- Procedura kontroli dokumentów i zapisów określająca cykl życia dokumentacji: tworzenie, weryfikację, autoryzację, wprowadzanie zmian, archiwizację i niszczenie. Zawiera zasady nadawania numerów wersji, prowadzenia rejestrów dokumentów oraz monitorowania ważności procedur,
- Metodologia szacowania ryzyka zawierająca sposób identyfikacji zagrożeń, oceny prawdopodobieństwa i skutków ewentualnych incydentów, a także określania priorytetów w zarządzaniu ryzykiem. Powinna opierać się na uznanych praktykach (np. ISO 27001) i być kompatybilna z wymaganiami Krajowych Ram Interoperacyjności / ustawy o Krajowym Systemie Cyberbezpieczeństwa.

b) Polityka Bezpieczeństwa Fizycznego, w tym dokumenty:

- Wzór ewidencji dostępu do pomieszczeń określający format i sposób prowadzenia rejestru wejść i wyjść z obszarów o ograniczonym dostępie. Pomaga monitorować i kontrolować ruch osobowy, minimalizując ryzyko nieautoryzowanego wejścia do stref chronionych (np. serwerownia, archiwum),
- Polityka kluczy definiująca zbiór zasad przydzielania, przechowywania i zwrotu kluczy (bądź kart dostępu) do pomieszczeń chronionych. Definiuje środki zapobiegawcze

(ewidencja, okresowa inwentaryzacja) i postępowanie w przypadku zagubienia/kradzieży kluczy,

- Wykaz pomieszczeń lub części pomieszczeń tworzących obszar przetwarzania danych określający listę pomieszczeń (lub stref) w których dochodzi do przetwarzania danych szczególnie chronionych. Określa kategorie dostępu i wymagane zabezpieczenia,
- Procedura dotycząca pracy w zabezpieczonych obszarach stanowiąca instrukcję postępowania dla personelu oraz osób zewnętrznych przebywających w obszarach o podwyższonym poziomie ochrony. Zawiera m.in. zasady weryfikacji tożsamości, konieczność rejestracji wizyt, dozwolone/zakazane działania (np. fotografowanie, nagrywanie),

c) Polityka Bezpieczeństwa Teleinformatycznego, w tym dokumenty:

- Procedura przechowywania, zbierania i zarządzania logami systemowymi ustalająca zasady pozyskiwania i analizy logów (z serwerów, urządzeń sieciowych, systemów operacyjnych), ich retencji (np. minimalny czas przechowywania), a także sposób wykrywania podejrzanych aktywności,
- Regulamin bezpieczeństwa informacji w pracy zdalnej określający zasady i wymagania dot. wykorzystywania sprzętu prywatnego lub służbowego poza siedzibą urzędu (np. VPN, szyfrowanie komunikacji, dwuskładnikowe uwierzytelnianie). Regulamin obejmuje również wskazówki dot. ochrony urządzeń mobilnych i reakcji na potencjalne zagrożenia,
- Instrukcje szyfrowania i bezpiecznego korzystania z przeglądarki zawierające wytyczne dotyczące wdrażania protokołów i narzędzi szyfrujących (SSL/TLS, S/MIME, VPN), konfiguracji przeglądarek, zarządzania certyfikatami, blokowania wtyczek podnoszących ryzyko ataku. Koncentrująca się na ochronie poufności i integralności przesyłanych informacji,
- Procedura przeglądów i konserwacji systemów określająca harmonogram i zakres regularnych prac utrzymaniowych (instalacja poprawek bezpieczeństwa, aktualizacja oprogramowania, kontrola poprawności działania usług),
- Raport pracy Administratora Systemów Informatycznych w postaci standardowego szablon dokumentu, w którym Administrator przedstawia okresowe czynności administracyjne (np. analiza logów, stanu antywirusów, aktualności certyfikatów). Umożliwia udokumentowanie i kontrolę zadań związanych z bezpieczeństwem teleinformatycznym,
- Procedura zarządzania incydentami bezpieczeństwa informacji i cyberbezpieczeństwo zawierająca kompleksowy opis trybu reagowania na ataki i naruszenia (phishing, ransomware, wyciek danych), obejmujący etapy zgłaszania, klasyfikacji, analizy, przeciwdziałania skutkom, a także obowiązek raportowania do organów zewnętrznych (np. CSIRT) w razie poważnych incydentów zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa,
- Procedura kontroli dostępu definiująca zasady nadawania i odbierania uprawnień w systemach IT, w tym autoryzacji użytkowników, polityki haseł, wykorzystania

tokenów lub kart inteligentnych. Przewidująca również sytuacje nadzwyczajne (np. udzielanie dostępu w trybie awaryjnym) i metodę kontroli skuteczności tych mechanizmów,

- Wzór formularza ewidencji sprzętu i oprogramowania umożliwiający bieżące śledzenie posiadanych urządzeń komputerowych (stacje robocze, laptopy, serwery, drukarki) oraz licencji na oprogramowanie. Zawiera pola na numer inwentarzowy, datę zakupu, rodzaj licencji, przypisanie do użytkownika, planowane terminy wymiany sprzętu itp.,
- Procedura szyfrowania danych określająca zasady i techniki zabezpieczenia danych w spoczynku (np. szyfrowanie dysków, pendrive'ów) i w tranzycie (np. poczta elektroniczna). Obejmująca również reguły przechowywania i ochrony kluczy kryptograficznych oraz sposób postępowania w przypadku utraty klucza lub hasła,
- Procedura zgłaszania, realizacji i testowania nowych rozwiązań informatycznych określająca pełny cykl wprowadzania nowych systemów i aplikacji (Change Management), obejmujący dokumentowanie celowości, ocenę ryzyka, testy bezpieczeństwa, wdrożenie produkcyjne oraz odbiór,
- Procedura użytkowania poczty elektronicznej oraz korzystania z sieci Internet zawierająca zbiór zaleceń nt. ochrony poczty przed phishingiem, spamem, złośliwym oprogramowaniem, a także wskazanie dozwolonych usług i zachowań w Internecie (np. blokada stron o podwyższonym ryzyku),
- Procedura utylizacji i niszczenia nośników danych precyzująca metody całkowitego niszczenia informacji przechowywanych na nośnikach papierowych i elektronicznych (dyski HDD, SSD, USB). Określa też protokół potwierdzający bezpowrotne i bezpieczne usunięcie danych, tak aby uniemożliwić ich odzyskanie,
- Procedura bezpieczeństwa sieci teleinformatycznych zawierająca zalecenia konfiguracyjne (firewalle, systemy IDS/IPS, segmentacja VLAN), sposób monitorowania ruchu sieciowego i reagowania na ataki (np. DDoS, sniffing). Uwzględnia zasady budowania bezpiecznej architektury i zarządzania punktami dostępu (Wi-Fi),
- Procedura postępowania w zakresie wykonywania i obsługi kopii zapasowych oraz testowania nośników służących do przechowywania informacji zawierająca szczegółowy opis planu wykonywania backupów, ich lokalizacji (on-site/off-site), częstotliwości testów przywracania danych, sposobu dokumentowania tych testów,
- Procedury zarządzania podatnościami opisująca cykliczny proces skanowania systemów i aplikacji w poszukiwaniu luk, priorytetyzacji działań naprawczych i weryfikacji poprawnego wdrożenia poprawek.

d) Polityka Ciągłości Działania, w tym dokumenty:

- Analizę wpływu biznesowego (BIA) polegająca na identyfikacji procesów kluczowych dla funkcjonowania jednostki, określeniu maksymalnych dopuszczalnych przestojów (RTO) i tolerancji na utratę danych (RPO), a także wskazanie zasobów krytycznych (personel, systemy IT, infrastruktura),

- Plany ciągłości działania zawierające szczegółowy opis procedur umożliwiających zachowanie lub szybkie przywrócenie kluczowych procesów w razie awarii, katastrofy naturalnej lub ataku cybernetycznego. Dokument ma uwzględniać także alternatywne miejsca pracy, sposoby komunikacji w kryzysie i priorytety w przywracaniu usług,
- Ewidencja testowania planów ciągłości działania zawierająca rejestr opisujący sposób i częstotliwość przeprowadzania testów, uwzględniając zastosowane scenariusze symulacyjne, wyniki testów, zidentyfikowane niezgodności oraz podjęte działania doskonalące,
- Raport ciągłości działania podsumowujący obecną dojrzałość organizacji w obszarze ciągłości działania, opisujący ewentualne incydenty, skuteczność.

e) Polityka Zarządzania Ryzykiem, w tym dokumenty:

- Procedura identyfikacji aktywów obejmująca kroki niezbędne do wykrywania i katalogowania zasobów informacyjnych jednostki.
- Procedura identyfikacji zagrożeń i podatności uwzględniająca metody rozpoznawania i klasyfikowania potencjalnych zagrożeń dla bezpieczeństwa informacji.
- Procedura analizy i oceny ryzyka opisująca sposoby oceny prawdopodobieństwa i wpływu zagrożeń na aktywa organizacji.
- Procedura określania akceptowalnego poziomu ryzyka definiująca kryteria dopuszczalnego ryzyka dla różnych procesów i zasobów.
- Procedura planu postępowania z ryzykiem prezentująca działania zmierzające do minimalizacji lub eliminacji zidentyfikowanych ryzyk.
- Procedura monitorowania i raportowania ryzyka dotyczy systematycznego nadzoru i informowania o stanie ryzyka w organizacji.

f) Polityka Szkoleń i Świadomości Pracowników. w tym dokumenty:

- Procedura identyfikacji potrzeb szkoleniowych obejmująca procesy wykrywania i określania wymagań szkoleniowych personelu w zakresie bezpieczeństwa informacji.
- Procedura wdrożeniowego szkolenia z bezpieczeństwa informacji opisująca działania związane z przeprowadzaniem szkoleń wstępnych dla nowych pracowników.
- Procedura szkoleń okresowych (cyklicznych) uwzględniająca planowanie i realizację regularnych szkoleń podnoszących świadomość bezpieczeństwa.
- Procedura testowania wiedzy i świadomości zawierająca metody oceny poziomu wiedzy pracowników oraz skuteczności prowadzonych szkoleń.
- Procedura prowadzenia kampanii informacyjnych opisująca działania komunikacyjne mające na celu zwiększenie świadomości w zakresie bezpieczeństwa informacji.
- Procedura prowadzenia rejestru szkoleń obejmująca ewidencjonowanie wszystkich działań szkoleniowych oraz udziału pracowników.

- Procedura oceny skuteczności szkoleń zawierająca sposoby mierzenia efektywności i wpływu prowadzonych działań edukacyjnych na poziom bezpieczeństwa informacji.

g) Opracowanie innych wymaganych polityk niewskazanych powyżej, a wynikających z przeprowadzonego audytu.

Wymagane jest, aby wszystkie opracowane polityki i procedury stanowiły część jednego, spójnego Systemu Zarządzania Bezpieczeństwem Informacji. System ten ma zapewniać skuteczne zarządzanie ryzykiem, reagowanie na incydenty, ochronę fizyczną i teleinformatyczną, a także nieprzerwane działanie kluczowych procesów jednostki.

Zaleca się także wskazania możliwej optymalizacji działań i procedur w zakresie bezpieczeństwa informacji oraz rekomendacji dotyczącej zasobów kadrowych niezbędnych do zarządzania systemami IT oraz SZBI.

3. Wdrożenie i praktyczne zastosowanie ma uporządkować procesy związane z bezpieczeństwem informacji oraz skuteczne zarządzać ryzykiem. Opracowane dokumenty mają być wdrożone w taki sposób, aby pracownicy, współpracownicy i dostawcy rozumieli i stosowali określone zasady. W ramach wdrożenia należy uwzględnić:

a) Omówienie opracowanej dokumentacji z osobami wdrażającymi SZBI oraz z kierownictwem,
b) Instrukcje postępowania (operacyjne) i materiały informacyjne,
c) Narzędzia wspierające (rejestry incydentów, wzory formularzy),
d) Opis wdrożonych elementów SZBI,
e) Wdrożenie procedury zgłaszania incydentów,
f) Wdrożenie Planu Ciągłości Działania (Business Continuity Plan, BCP),
g) Wdrożenie Planu Odzyskiwania po Awarii (Disaster Recovery Plan, DRP),
h) Przeprowadzenie niezbędnych testów, pozwalających ocenić skuteczność wdrożonych rozwiązań,
i) Przekazanie materiałów szkoleniowych kierownikowi oraz pracownikom Centrum Informatycznego (np. prezentacji, skryptów) oraz metod oceny skuteczności (testów, ankiet),
j) Opracowanie i przeprowadzenie szkolenia dla pracowników Centrum Informatycznego oraz osób powiązanych (minimalnie 12 osób w wymiarze 20 godzin lekcyjnych),
k) Opracowanie i przeprowadzenie szkolenia dla kadry kierowniczej (minimalnie 12 osób w wymiarze 8 godzin lekcyjnych),
l) Opracowanie kursu e-learningowego (bez nauczyciela) dla pracowników administracji zamawiającego z zakresu SZBI w ramach systemu Moodle (w wymiarze 3 godzin zegarowych pracy własnej),
m) Opracowanie kursu e-learningowego (bez nauczyciela) dla nauczycieli akademickich Zamawiającego z zakresu SZBI w ramach systemu Moodle (w wymiarze 2 godzin zegarowych pracy własnej),
n) Dodatkowo Wykonawca zobowiązany jest do przygotowania w porozumieniu z Zamawiającym postępowania o certyfikację ISO 27001.

4. Przegląd, testowanie i aktualizacja pozwolą na ocenę skuteczności zastosowanych zabezpieczeń oraz zapewnią ciągłe doskonalenie systemu. Po wdrożeniu dokumentacji konieczne jest zaplanowanie i wykonanie:

a) Audytu końcowego celem sprawdzenia, czy wdrożony SZBI spełnia wymagania Normy i czy jest gotowy do certyfikacji. Audyt ma wskazać zgodność z Normą, nieprawidłowości i możliwości poprawy oraz identyfikację przyczyn błędów, aby wyeliminować je przed audytem certyfikującym,
b) Przeglądu skuteczności SZBI wraz z pomiarem skuteczności zastosowanych zabezpieczeń, przegląd szacowania ryzyka wraz z aktualizacją,
c) Testów, symulacji incydentów i planów ciągłości działania, dzięki którym będzie można wykryć ewentualne niezgodności, niedostatki i wprowadzić działania korygujące,
d) Raportu z przeprowadzonych testów i audytów: dokumentację wykonanych prac, analizę wyników testów penetracyjnych i zabezpieczeń serwisów oraz zalecenia i wnioski,
e) Wsparcia Zamawiającego w analizie raportu końcowego i wdrożeniu rekomendacji poaudytowych – w szczególności poprzez aktualizację dokumentacji SZBI, zaplanowanie działań korygujących i zapobiegawczych w obszarach wskazanych w raporcie oraz przeprowadzenie ponownych testów wybranych elementów, jeśli będzie to konieczne dla potwierdzenia usunięcia zidentyfikowanych podatności.

5. Opracowanie raportu końcowego i przekazanie dokumentacji

a) Wykonawca dostarczy raport podsumowujący (w formie papierowej i elektronicznej wraz z prawami autorskimi majątkowymi) zawierający opis wykonanych prac, zalecenia i opis potencjalnych obszarów do dalszego rozwoju.
b) Odbiór zostanie potwierdzony podpisaniem protokołu, w którym Zamawiający oświadcza, że zakres przedmiotu zamówienia został zrealizowany należycie.
c) Zamawiający oczekuje wsparcia przy audycie certyfikującym celem uzyskania akredytowanego certyfikatu z ISO 27001, w tym komunikacja z akredytowaną jednostką certyfikującą, aby pomóc w ustaleniu wszystkich spraw związanych z certyfikacją ISO 27001.
d) Wykonanie, wspólnie z Zamawiającym, działań poaudytowych w formie uzgodnionej z Zamawiającym oraz dokonanie korekty dokumentacji, o ile okaże się to konieczne.

Postanowienia końcowe

Wykonawca jest zobowiązany do zachowania w poufności wszystkich informacji, danych i dokumentów pozyskanych podczas realizacji niniejszego zamówienia; zobowiązanie to obejmuje zakaz ujawniania treści wrażliwych osobom lub podmiotom nieupoważnionym i obowiązuje także po zakończeniu współpracy, o ile przepisy prawa lub umowa nie stanowią inaczej. Z chwilą odbioru końcowych rezultatów prac wszelkie wytworzone materiały i dokumenty przechodzą na własność Zamawiającego wraz z przysługującymi im majątkowymi prawami autorskimi. W razie pojawienia się w trakcie realizacji zamówienia nowych regulacji krajowych lub unijnych, Wykonawca uwzględni te zmiany w tworzonej dokumentacji i procedurach, tak aby zapewnić ciągłą zgodność z obowiązującym prawem. Szczegółowe ustalenia dotyczące kar umownych za opóźnienia, nienależyte wykonanie przedmiotu zamówienia, czy naruszenie tajemnicy, a także zasady odpowiedzialności stron, zostaną sprecyzowane w umowie.