Katalog obligatoryjnych zabezpieczeń i kontroli na podstawie załącznika A do normy ISO27001-2022

8	Kontrole technologiczne	
8.2	Uprzywilejowane prawa dostępu	Przydzielanie i wykorzystanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować. *Dostawca zapewni, że możliwe jest przydzielanie zróżnicowanych pra dostępu i że w każdym czasie możliwy jest audyt przydzielonych uprawnień do osób wraz z ich rejestrem logowania*
8.3	Ograniczenie dostępu do informacji	Dostęp do informacji oraz powiązanych aktywów należy ograniczać zgodnie z polityką kontroli dostępu. *Dostawca zapewni, że możliwe jest ograniczanie widoczności informacji w systemie w zależności od przydzielonych uprawnień (ograniczenie dostępu do informacji)*
8.4	Dostęp do kodów źródłowych	Dostęp do odczytu i zapisu kodu źródłowego, narzędzi programistycznych i bibliotek oprogramowania powinien być odpowiednio zarządzany. *Dostawca zapewni, że dostęp do kodu źródłowego aplikacji nie jest dostępny podczas używania programu (np. przy użyciu przeglądarki internetowej itp.)*
8.5	Bezpieczne uwierzytelnienie	Bezpieczne technologie i procedury uwierzytelnienia powinny być wdrażane w oparciu o ograniczenia w dostępie do informacji oraz tematyczną (obszarową) politykę kontroli dostępu. *Dostawca zapewni rozdział uprawnień dla każdego modułu niezależnie, logowanie po parametrach uwierzytelniających do danych osobowych dodatkowo.*
8.9	Zarządzanie konfiguracją	Konfiguracje, w tym konfiguracje zabezpieczeń, sprzętu, oprogramowania, usług i sieci powinny być ustanowione, udokumentowane, wdrożone, monitorowane i przeglądane. *Dostawca dostarczy w ramach umowy szczegółową dokumentację techniczną zawierająca informacje o architekturze systemu, bazie danych, repozytoriach plików, wykorzystanych językach programowania i frameworkach oraz innych aspektach technicznych wraz z ich dokładną konfiguracją umożliwiającą odtworzenie na środowisku zamawiającego*.

8.10	Usuwanie informacji	Informacje przechowywane w systemach informatycznych, urządzeniach lub na innych nośnikach danych powinny być usuwane, gdy nie są już potrzebne. *Dostawca zapewni w systemie pole lub pola (atrybuty danych) dla każdego rekordy danych w oparciu o które*

		możliwe jest ustawienie polityki retencji danych w systemie oraz Dostawca zapewni mechanizmy masowego usuwania danych w systemie lub ich anonimizacji zgodnie z zadanymi w systemie regułami opartymi o w/w pola.
8.11	Maskowanie danych	Maskowanie danych powinno być stosowane zgodnie z polityką tematyczną organizacji dotyczącą kontroli dostępu i innymi powiązanymi politykami specyficznymi dla danego tematu oraz wymaganiami biznesowymi, z uwzględnieniem obowiązujących przepisów. *Dostawca zapewni w systemie mechanizmy masowania wybranych rekordów danych zależnie od kryteriów rodzajowych, daty, oraz innych ustalonych z Zamawiającym atrybutów.*
8.13	Zapasowe kopie bezpieczeństwa	Zapasowe kopie informacji, oprogramowania i obrazów systemów należy regularnie wykonywać i testować, zgodnie z ustaloną polityką kopii zapasowych. *Dostawca zapewni w systemie mechanizmy wykonywania i odtwarzania oraz testowania kopii zapasowych systemu według zadanego harmonogramu.*
8.15	Rejestrowanie działań	Należy tworzyć, przechowywać, chronić i analizować dzienniki rejestrujące działania, wyjątki, usterki i inne istotne zdarzenia. *Dostawca przygotuje w systemie rejestrowanie w pliku logów każdej czynności wykonanej przez każdego użytkownika oraz przez mechanizmy systemowe w odpowiednim logu, który możliwy jest do odczytu poza systemem bez konieczności logowania do systemu (np. W przypadku awarii systemu logi musza być możliwe do odczytania.*

8.24	Użycie kryptografii	Należy określić i wdrożyć zasady efektywnego wykorzystania kryptografii, w tym zarządzania kluczami kryptograficznymi. *Dostawca w dokumentacji uwzględni wszystkie wykorzystane metody kryptograficzne w systemie*
8.25	Bezpieczeństwo prac rozwojowych	Należy ustanowić zasady prac nad rozwojem oprogramowania i systemów oraz stosować je w pracach rozwojowych prowadzonych wewnątrz organizacji. *Przed rozpoczęciem prac dostawca przedstawi opis bezpieczeństwa prac rozwojowych nad oprogramowaniem z zachowaniem:* *Poufności* *Praw autorskich* *Dostępu do danych Zamawiającego* *Dostępu do danych użytkowników Zamawiającego.* *Przedstawione metody musza zostać zaakceptowane przez Zamawiającego.*
8.28	Bezpieczne kodowanie	Podczas tworzenia oprogramowania należy stosować zasady bezpiecznego kodowania. *Dostawca zastosuje metody bezpiecznego kodowania*

8.29	Testowanie bezpieczeństwa w fazie rozwoju i akceptacja	Procesy testowania bezpieczeństwa powinny być zdefiniowane i wdrożone w cyklu rozwojowym oprogramowania.
8.30	Outsourcing prac rozwojowych	Organizacja powinna nadzorować i monitorować prace rozwojowe nad systemami zlecone podmiotom zewnętrznym. *Dostawca wyraża zgodę w każdym czasie podczas trwania umowy na audyt i nadzór nad cyklem prac rozwojowych w miejscu ich wykonywania po uprzednim zawiadomieniu przez Zamawiającego z terminem 7 dniu roboczych.*
8.31	Rozdzielenie środowisk deweloperskich, testowych i produkcyjnych	Środowiska programistyczne, testowe i produkcyjne powinny być rozdzielone i zabezpieczone. *Dostawca przed rozpoczęciem prac rozdzieli środowiska programistyczne i testowe od produkcyjnego i przedstawi raport z tej czynności Zamawiającemu.*
8.32	Zarządzanie zmianami	Zmiany w urządzeniach do przetwarzania informacji i systemach informatycznych powinny podlegać procedurom zarządzania zmianami. *Dostawca wykona szczegółową dokumentację zmian w oprogramowaniu i przedstawi tę dokumentację jak efekt wykonanych prac przed rozliczeniem.*
8.33	Ochrona danych testowych	Dane testowe należy starannie wybierać, chronić i nadzorować. *Dostawca przygotuje we własnym zakresie dane testowe które nie są danymi rzeczywistymi i nie zawierają żadnych elementów chronionych.*
8.34	Ochrona systemów informatycznych podczas testów audytowych	Testy audytowe i inne działania zapewniające pewność, obejmujące ocenę systemów operacyjnych, powinny być planowane i uzgadniane między testerem a odpowiednim kierownictwem. *Dostawca uzgodni termin i czas wykonywania wszelkich prac nad system Zamawiającego w tym testów, sprawdzeń poprawek i konfiguracji oraz testów bezpieczeństwa.*