

### Opis przedmiotu zamówienia

Przedmiotem umowy jest dostawa systemu do automatyzacji zarządzania infrastrukturą informatyczną oraz oprogramowaniem wraz z dostawą licencji zwanym dalej Systemem Automatyzacji, wdrożeniem dostarczonego oprogramowania, asystą techniczną, dokumentacją projektową, dostępem do dokumentacji produktu oraz szkoleniem dla pracowników Zamawiającego oraz przeniesienie lub adaptacja stworzonych przez Zamawiającego już istniejących playbook-ów i ról w ramach użytkowanego dotychczas oprogramowania do automatyzacji zarządzania infrastrukturą i oprogramowaniem Ansible w wersji 2.9.16 i 2.15.8.

#### Szczegóły opisu przedmiotu zamówienia:

##### 1. Wymagania do Systemu Automatyzacji

Nazwa	Wymagania minimalne:
Licencja	<ul style="list-style-type: none"><li>1.1. Licencja dla 200 zarządzanych urządzeń;</li><li>1.2. Licencja na okres 12 miesięcy;</li><li>1.3. Zamawiający wymaga dostarczenia licencji na system operacyjny rekomendowany przez producenta oprogramowania, jeżeli dostarczone oprogramowanie będzie tego wymagało wraz niezbędnym wsparciem w zakresie aktualizacji i utrzymania systemu oraz gwarancją w okresie 12 miesięcy w ilości niezbędnej do jego instalacji;</li><li>1.4. Rozwiązanie musi zawierać wszystkie niezbędne licencje do uruchomienia opisanych funkcjonalności, włączając w to licencje na system operacyjny – jeżeli takie są niezbędne do jego uruchomienia;</li></ul>
Cechy oprogramowania	<p>Rozwiązanie posiada wsparcie techniczne w języku polskim lub angielskim;</p> <p>Oferowane oprogramowanie:</p>

	<p>1.5. musi umożliwiać automatyzację administracji, w tym procesów instalacji, konfiguracji i modyfikacji dla środowisk różnych producentów:</p> <ul style="list-style-type: none"> <li>1.5.1. VMware dla oprogramowania VMware vSphere 7 i 8 Enterprise Plus;</li> <li>1.5.2. Kubernetes jako otwarta platforma do skalowania aplikacji kontenerowych;</li> <li>1.5.3. Macierzy dyskowych firmy NetApp;</li> <li>1.5.4. Systemów operacyjnych klasy Linux/Unix/Windows;</li> <li>1.5.5. Przełączników sieciowych firm: Juniper, HP (w ramach dostępu po SSH i SNMP);</li> <li>1.5.6. Urządzeń Big IP f5;</li> <li>1.5.7. Systemu backupu Commvault;</li> </ul> <p>1.6. musi posiadać centralny interfejs Web umożliwiający:</p> <ul style="list-style-type: none"> <li>1.6.1. bezagentowe zarządzanie konfiguracją elementów infrastruktury informatycznej, wchodzących w skład rozwiązań wskazanych w poprzednim punkcie, na podstawie algorytmów/procesów wyrażonych w plikach typu tekstowego ze strukturą drzewa uporządkowanego przeznaczonych do reprezentowania różnych danych w ustrukturyzowany sposób, np. YAML lub JSON, z możliwością podania dodatkowych parametrów wywołania takiego algorytmu/procesu;</li> <li>1.6.2. zarządzanie przydziałem dostępu w oparciu o role i grupy;</li> <li>1.6.3. zarządzanie harmonogramowaniem zadań i wysyłaniem powiadomień o ich realizacji;</li> <li>1.6.4. zarządzanie danymi dostępowymi umożliwiającymi wywoływanie czynności konfiguracyjnych na zarządzanych elementach (urządzeniach, systemach, usługach itp.);</li> <li>1.6.5. Systemu Automatyzacji musi być zgodny z wytycznymi WCAG minimum 2.1</li> </ul> <p>1.7. musi umożliwiać szyfrowanie (przy przechowywaniu) i ukrywanie (uniemożliwienie wyświetlenia) wszystkich</p>
--	---

	<p>stosowanych danych uwierzytelniających: zarówno danych dostępu do zarządzanych elementów, jak i danych stanowiących część konfiguracji zarządzanych elementów;</p> <p>1.8. musi zapewniać szyfrowanie połączenia do każdego zarządzanego elementu;</p> <p>1.9. musi posiadać mechanizm REST ful API do integracji z zewnętrznymi elementami środowiska informatycznego oraz możliwość zarządzania z linii poleceń (CLI);</p> <p>1.10. musi działać bez instalacji agentów na elementach zarządzanych;</p> <p>1.11. musi pozwalać na wykonywanie poleceń ad-hoc, jak i uruchamianie zadań na podstawie przygotowanych wcześniej deklaracji w plikach typu JSON lub YAML przechowywanych w repozytorium;</p> <p>1.12. musi logować działania użytkowników oraz przebieg harmonogramowanych działań;</p> <p>1.13. musi umożliwiać zbieranie informacji o każdym zarządzanym elemencie;</p> <p>1.14. musi umożliwiać zapis zdarzeń systemowych na zewnętrznym serwerze syslog i umożliwiać wysyłanie zdarzeń i powiadomień do systemów klasy SIEM (Zamawiający wykorzystuje system Splunk Enterprise oraz Sentinel);</p> <p>1.15. możliwość umieszczenia baz, o ile oferowane rozwiązanie wymagać będzie stosowania baz danych, na osobnym dedykowanym serwerze bazodanowym;</p> <p>1.16. musi być zainstalowane i uruchomione na platformie wirtualnej w systemie Linux w systemie virtualizacji VMware;</p> <p>1.17. musi być niezależne od zastosowanej infrastruktury sprzętowej, na której zostanie zainstalowane i uruchomione;</p> <p>1.18. wymagane jest udokumentowane wsparcie producenta oferowanego rozwiązania dla zastosowanego systemu operacyjnego/platformy, na którym zostanie zainstalowane i uruchomione oferowane rozwiązanie;</p> <p>1.19. musi wspierać rozwiązania wysokiej dostępności, pozwalać na instalacje w trybie klastra (HA);</p>
--	---

	<p>1.20. musi pozwalać na skalowanie wszcz, dla zachowania wydajności rozwiązania w różnych segmentach zarządzanego środowiska informatycznego;</p> <p>1.21. musi pozwalać na definiowanie algorytmów i parametrów automatyzowanych procesów w standardowym formacie takim jak JSON, YAML;</p> <p>1.22. musi wspierać uwierzytelnianie użytkowników za pomocą mechanizmów: wbudowanego uwierzytelniania, LDAP, SAML, OpenID Connect. Zamawiający korzysta z identity providera Entra ID (dawniej AzureAD);</p> <p>1.23. musi umożliwiać wysyłkę powiadomień poprzez e-mail (np. o nieprawidłowym logowaniu lub wykonaniu harmonogramu dla grupy hostów);</p> <p>1.24. musi posiadać możliwość połączenia działania kilku algorytmów/procesów w jeden algorytm/proces;</p> <p>1.25. musi posiadać mechanizm integracji – pobierania danych dostępowych – z systemami: HashiCorp Vault, CyberArk AIM, CyberArk Conjur, Microsoft Azure Key Vault;</p> <p>1.26. wymagane jest wsparcie dla generowania metryk elementów oferowanego rozwiązania za pomocą standardowych protokołów np. Prometheus;</p> <p>1.27. musi umożliwiać integrację z repozytoriami Git w których przechowywane są algorytmy automatyzacji;</p> <p>1.28. musi zapewniać dostęp do modułów napisanych przez autoryzowanych dostawców (w szczególności Microsoft, Vmware, F5 BIG-IP, NetApp) przeznaczonych do zarządzania ich produktami.</p>
Gwarancja Producenta	<p>Gwarancja producenta obejmuje:</p> <p>1.29. Minimum 12 miesięcy gwarancji producenta rozwiązania.</p> <p>1.30. Zapewnia możliwość pobierania i użytkowania aktualizacji i poprawek oprogramowania.</p> <p>1.31. Zapewnia dostępność każdej obecnej i przyszłej wersji oprogramowania w ramach subskrypcji bez dodatkowych opłat.</p> <p>1.32. Zapewnia możliwość zgłaszania wad w oprogramowaniu za pomocą oficjalnych kanałów komunikacji producenta.</p>

	<p>1.33. Zapewnia dostęp do bazy wiedzy zawierającej rozpoznane i rozwiązane problemy, artykuły eksperckie oraz pełną dokumentację techniczną.</p> <p>Wsparcie techniczne Wykonawcy w okresie minimum 12 miesięcy:</p> <p>1.34. Wsparcie wykonawcy będzie świadczone co najmniej w dni robocze Zamawiającego od poniedziałku do piątku z wyłączeniem ustawowo dni wolnych od pracy w godz. 8.00-16.00, w języku polskim lub angielskim przez cały okres obowiązywania gwarancji.</p> <p>1.35. Wsparcie z zakresu działania i konfiguracji zadań realizowanych przez dostarczone Oprogramowanie Wykonawca musi rozwiązać w ciągu 7 dni roboczych, a w przypadku problemu związanego z dostarczonym oprogramowaniem przez producenta na zasadach standardowej gwarancji.</p>
Warunki wsparcia technicznego Wykonawcy	<p>Wsparcie techniczne Wykonawcy w okresie minimum 12 miesięcy:</p> <p>1.36. Wsparcie wykonawcy będzie świadczone co najmniej w dni robocze Zamawiającego od poniedziałku do piątku z wyłączeniem ustawowo dni wolnych od pracy w godz. 8.00-16.00, w języku polskim lub angielskim przez cały okres obowiązywania gwarancji.</p> <p>1.37. Wsparcie z zakresu działania i konfiguracji zadań realizowanych przez dostarczone Oprogramowanie Wykonawca musi rozwiązać w ciągu 7 dni roboczych, a w przypadku problemu związanego z dostarczonym oprogramowaniem przez producenta na zasadach standardowej gwarancji.</p>
Warunki Asysty Technicznej	<p>1.38. Wykonawca zobowiązuje się do wykonywania na rzecz Zamawiającego prac o charakterze Asysty Technicznej w wymiarze do 24 roboczogodzin w okresie realizacji Umowy.</p> <p>Asysta Techniczna obejmuje:</p> <p>1.38.1. Konsultacje i pomoc udzielaną przez Konsultanta w siedzibie Zamawiającego bądź zdalnie przez personel</p>

	<p>Wykonawcy w zakresie wdrażanego oprogramowania i przy rozwijaniu algorytmów automatyzacji.</p> <p>1.38.2. Modyfikacje i rekonfiguracje Systemu w ramach nowych funkcjonalności Systemu w terminie ustalonym pomiędzy stronami.</p> <p>1.38.3. Integracje z nowymi źródłami danych.</p>
--	---

## 2. Wdrożenie

### 2.1. Dostarczenie oprogramowania i instalacja

Wykonawca dokona instalacji i konfiguracji wszystkich niezbędnych do wdrożenia komponentów oprogramowania w siedzibie Zamawiającego w środowisku VMware vSphere 7 Zamawiającego na przygotowanych po wcześniejszych uzgodnieniach z Wykonawcą maszynach wirtualnych.

### 2.2. Konfiguracja obejmuje: Integrację uwierzytelniania użytkowników z Microsoft Entra ID (konfigurację po stronie Azure realizuje Zamawiający, po stronie Oprogramowania Wykonawca).

2.2.1. Integrację uwierzytelniania dodatkowych użytkowników z AD (wydzielona grupa użytkowników uprawnionych do dostępu do interfejsu Oprogramowania w przypadku braku połączenia z Entra ID).

2.2.2. Utworzenie (jeżeli nie istnieje) i skonfigurowanie lokalnego konta administratora do zarządzania w razie awarii uwierzytelniania zdalnego lub innych prac przy aplikacji wymagających wyższych uprawnień.

2.2.3. Dostarczenie i implementacja wzorcowych algorytmów/zadań zbierających fakty z urządzeń zarządzanych (Linux, Windows, macierz NetApp, przełącznik Juniper, przełącznik HP, Big IP f5, Commvault) i zademonstrowanie połączenia do każdego typu urządzenia na środowisku Zamawiającego.

2.2.4. Przygotowanie inventory (definicji zbioru zarządzanych urządzeń): Statycznego dla urządzeń fizycznych według listy dostarczonej przez Zamawiającego, Dynamicznego dla maszyn wirtualnych Vmware.

2.2.5. Integracja platformy web do zarządzania rozwiązaniem z wykorzystaniem repozytoriów Git Zamawiającego, w których przechowywany jest kod algorytmów i parametrów automatyzowanych procesów.

2.2.6. Ustawienie uprawnień poszczególnych ról po konsultacji z Zamawiającym,

2.2.7. Przypisanie uprawnień poszczególnym użytkownikom po konsultacji z Zamawiającym.

2.2.8. Wykonanie wspólnie z Zamawiającym przeglądu i akceptacji wdrożonego rozwiązania pod kątem bezpieczeństwa oraz jego hardening zgodnie z najlepszymi praktykami.

2.3. Przygotowanie i implementacja dodatkowych algorytmów zadań do zarządzania środowiskiem wirtualnym

Nazwa	Opis
Tworzenie nowej maszyny Oracle/Debian Linux na podstawie template - interaktywny	Tworzenie maszyny wirtualnej Vmware na platformie na podstawie gotowego szablonu Vmware. Formularz powinien zawierać domyślne parametry maszyny z możliwością wprowadzania własnych parametrów (wybór szablonu, procesory, RAM, wielkość partycji, VLAN).
Tworzenie nowej maszyny Oracle/Debian Linux na podstawie template – na podstawie pliku yaml	Tworzenie maszyny wirtualnej Vmware na podstawie gotowego szablonu Vmware, z konfiguracją określoną w pliku yaml. Możliwość jednoczesnego tworzenia większej liczby wirtualnych maszyn.
Zarządzanie hasłami w Keepass	Zarządzanie (dodawanie/usuwanie/modyfikacja) hasłami przechowywanymi w aplikacji Keepass – działający proof-of-concept do wykorzystania w zadaniach konfiguracyjnych zasoby chronione hasłem.
Tagowanie Serwerów	Tagowanie serwerów w Vmware w celu tworzenia grup. Poprzez tagowanie Zamawiający rozumie zmianę wskazanych atrybutów.
Utwardzanie (hardening) systemu operacyjnego Linux	Przygotowanie procesu konfiguracji systemu wg założeń określonych przez Zamawiającego.
Zarządzanie firewallem (iptables)	Otwieranie i zamykanie dostępu do maszyny na poszczególnych portach i opcjonalnie z zadanych adresów źródłowych. Możliwość wywołania: - interaktywnego, z formularzem wyboru serwera, zbierającego i prezentującego informacje o konfiguracji firewalla - interaktywnego, z formularzem wyboru serwera i wprowadzanej/usuwanej reguły firewalla - nieinteraktywnego, nakładającego konfigurację określoną w pliku yaml

Obsługa wysyłki konfiguracji serwerów Linux do repozytorium Git	<p>Dodawanie i/lub usuwanie wybranych elementów konfiguracji serwera do zdalnego repozytorium git-a:</p> <p>Tworzenie przez API serwisu Gitea repozytorium dedykowanego serwerowi,</p> <p>Wybór zapisywanych w repozytorium plików na podstawie listy w pliku yaml,</p> <p>Konfiguracja okresowej (cron) wysyłki konfiguracji do zdalnego repozytorium</p>
Zarządzanie lokalnymi kontami użytkowników Linux	Zakładanie/usuwanie/zarządzanie kontami użytkowników (oraz wgrywanie/usuwanie/aktualizacja ich kluczy publicznych ssh na podstawie konfiguracji w plikach yaml)
Konfiguracja sudo	Zarządzanie wpisami sudo (dodawanie, usuwanie, listowanie, zmiana uprawnień) dla wybranego/wybranych użytkowników na podstawie konfiguracji w plikach yaml
Zarządzanie wpisami w phpIPAM	Zarządzanie (dodawanie/usuwanie/modyfikacja) wpisów serwerów w aplikacji phpIPAM (API).
Instalacja i konfiguracja agenta Zabbix na serwerze	Instalacja agenta (możliwość wyboru wersji) oraz jego konfiguracja. Możliwość zmiany gałęzi repozytorium do wyższej na już zainstalowanych serwerach.
Zarządzanie monitorowanymi serwerami w Zabbix Serwer	Dodawanie/Usuwanie serwera do monitorowania. Dodawanie szablonów (template-ów) Zabbixa do monitorowania usług zadeklarowanych w plikach yaml. Możliwość wyboru sposobu zabezpieczenia komunikacji poprzez klucz PSK lub certyfikat.
Zmiana wersji agenta Zabbix	Zmiana wersji agenta, usunięcie starej wersji, konfiguracja agenta oraz zmiany w konfiguracji po stronie serwera (wymiany szablonu)
Konfiguracja monitoringu na serwerze Nagios	Dodawania/usuwanie serwerów do monitorowania (ICMP, ważność certyfikatów, zajętość dysków, działanie usług zadeklarowanych w plikach yaml).
Instalacja i konfiguracja agenta Nagios	Instalacja agenta Nagios, jego konfiguracja i ewentualnie instalacja i konfiguracja pluginów
Antywirus Microsoft Defender for endpoint	Instalacja/usuwanie agenta – onboarding/offboarding



Konfiguracja serwera czasu na serwerach	Konfiguracja serwera czasu na serwer Chronyd Zamawiającego oraz strefę czasową Europe/Warsaw.
Konfiguracja usługi rsyslog	Dodanie/modyfikacja wymaganych wpisów w głównym pliku konfiguracyjnym, wgranie szablonów do wysyłki logów z aplikacji (nginx, apache2, php, php-fpm, mariadb, postgresql).
Konfiguracja logrotate	Konfiguracja domyślnych ustawień logrotate (np. domyślnie włączona kompresja, rotowanie logów dzienne, okres ostatnie 14 dni).
Zarządzanie logrotate	Wgranie wybranych szablonów do rotowania logów aplikacji (np. nginx, apache2, php, php-fpm, mariadb, postgresql)
Certificate Signing Request	Generowanie pary kluczy i CSR na zarządzanym urządzeniu.
Certyfikat zdalny	Generowanie certyfikatów na podstawie CSR u zewnętrznego dostawcy Sectigo (API).
Certyfikat lokalny	Generowanie certyfikatów na podstawie CSR i importowanie ich od lokalnego centralnego CA (Active Directory Certificate Services).
Zarządzanie DNS	Zarządzanie (dodawanie, usuwanie, zmiana) wpisami w usłudze działającej w systemie Linux „DNS Bind”, wysłanie zmian do git.
Instalacja wybranych aplikacji	Instalacja i konfiguracja aplikacji (nginx, apache2, php, php-fpm, mariadb, postgresql) wraz z podstawową konfiguracją zakres obejmuje: instalację aplikacji, konfigurację pobraną z szablonu aplikacji pobranego z Git.
Zarządzanie grupami w Active Directory	Dodawanie/usuwanie użytkowników do grup na poziomie Active Directory.
Snapshot serwera	Wykonanie/usunięcie/przywrócenie snapshot-u maszyny w VMware

#### 2.4. Przygotowanie i implementacja zbiorczych algorytmów zadań jako procedur uruchamiających zestaw pojedynczych algorytmów zadań

Nazwa	Opis
Instalacja nowej maszyny	Wykonanie zadań na podstawie konfiguracji w yaml lub interaktywnie, z użyciem formularzy web:

	<p>2.4.1. Tworzenie nowej maszyny Linux na podstawie template-u Vmware;</p> <p>2.4.2. Hardening systemu operacyjnego;</p> <p>2.4.3. Konfiguracja firewalla;</p> <p>2.4.4. Dodanie do śledzenia wybranych plików konfiguracyjnych /etc do git-a i wysyłka do zdalnego repozytorium;</p> <p>2.4.5. Utworzenie lokalnych kont dla wybranych administratorów;</p> <p>2.4.6. Dodanie wpisu w phpIPAM;</p> <p>2.4.7. Dodanie wpisu w DNS;</p> <p>2.4.8. Zapisanie hasła root-a w centralnym spisie haseł administratorów</p> <p>2.4.9. Instalacja i konfiguracja agenta Zabbix-a oraz dodanie wpisu o nowym serwerze na Zabbix Server;</p> <p>2.4.10. Instalacja i konfiguracja Antywirus Defender;</p> <p>2.4.11. Konfiguracja sudo dla wybranych użytkowników;</p> <p>2.4.12. Konfiguracja usługi sshd;</p> <p>2.4.13. Konfiguracja usługi rsyslog;</p> <p>2.4.14. Konfiguracja logrotate;</p> <p>2.4.15. Instalacja i konfiguracja agenta Nagios oraz dodanie wpisu o nowym serwerze na Nagios Server.</p> <p>2.4.16. W przypadku zadeklarowania w pliku yaml instalacji wybranych aplikacji:</p> <p>2.4.16.1. Przygotowanie certyfikatu – jeśli aplikacja tego wymaga;</p> <p>2.4.16.2. Instalacja i konfiguracja aplikacji;</p> <p>2.4.16.3. Konfiguracja firewalla dla danej aplikacji;</p> <p>2.4.16.4. Konfiguracja rsyslog i logrotate dla danej aplikacji;</p> <p>2.4.16.5. Konfiguracja monitoringu Zabbix i/lub Nagios dla danej aplikacji;</p> <p>W przypadku problemów na którymś z etapów, możliwość wycofania dokonanych zmian.</p>
Usuwanie maszyny	Usunięcie serwera z Vmware oraz wszelkich wpisów z innych systemów (DNS, monitoring Zabbix/Nagios, phpIPAM), archiwizacja repozytorium Git.

Zarządzanie systemem USOS	Uniwersytecki System Obsługi Studentów – przeniesienie/adaptacja playbook-ów i ról stworzonych obecnie w technologii Ansible (ok. 100 ról konfigurujących ok. 25 usług).
---------------------------	--

### 3. Szkolenie

Szkolenie z administracji wdrażanym oprogramowaniem dla pracowników Zamawiającego, które odbędzie się w formie zdalnej dla 20 pracowników Zamawiającego. Czas trwania szkolenia 2 dni (16 godzin łącznie). Szkolenie zostanie potwierdzone podpisaniem przez dwie strony protokołem odbioru.

### 4. Procedury odbioru

#### 4.1. Zasady ogólne

4.1.1. Odbiór prac wykonanych w trakcie realizacji polega na weryfikacji, czy przedmiot odbioru spełnia wymagania określone z uwzględnieniem szczegółowych wymagań określonych w toku współpracy Stron.

#### 4.2. Procedura odbioru Dokumentacji Projektowej

4.2.1. W terminie wskazanym w umowie, Wykonawca prześle poszczególne produkty Dokumentacji Projektowej. Zamawiający potwierdzi przekazanie dokumentacji projektowej w momencie jej otrzymania poprzez podpisane protokołu odbioru.

#### 4.3. Procedura odbioru Systemu Automatyzacji:

4.3.1. Wykonawca zgłasza System Automatyzacji do odbioru poprzez przekazanie podpisanego protokołu odbioru.

4.3.2. Podstawą weryfikacji Systemu Automatyzacji do odbioru będzie:

4.3.2.1. Wykonanie testów akceptacyjnych określonych w poniższym planie testów.

4.3.2.2. Testy akceptacyjne przeprowadza Wykonawca na środowisku u Zamawiającego. Nadzór nad Testami Akceptacyjnymi sprawuje Zamawiający. W Testach Akceptacyjnych uczestniczą przedstawiciele Zamawiającego i Wykonawcy.

4.3.2.3. Testy akceptacyjne przeprowadzone zostaną w ramach maksymalnie trzech tur, trwających max. 5 dni roboczych dla każdej z tur, pomiędzy którymi Wykonawca będzie dokonywał wgrywania poprawek do błędów zgłoszonych w czasie przeprowadzonych testów akceptacyjnych. Przerwa pomiędzy turami testów akceptacyjnych nie może być dłuższa niż 2 dni robocze.

- 4.3.2.4. Pierwsza tura polegać będzie na przeprowadzeniu wszystkich uzgodnionych w planie testów akceptacyjnych scenariuszy testowych.
- 4.3.2.5. Druga tura odbędzie się, jeżeli podczas pierwszej tury zostały wykryte błędy. Obejmować będzie przeprowadzenie scenariuszy testowych, które w pierwszej turze zakończyły się niepowodzeniem oraz wykonanie scenariuszy testowych (w ramach testów regresyjnych) dla funkcjonalności, na które poprawki mogły mieć wpływ.
- 4.3.2.6. Trzecia tura odbędzie się, jeżeli podczas drugiej tury zostały wykryte błędy. Obejmować będzie przeprowadzenie scenariuszy testowych, które w drugiej turze zakończyły się niepowodzeniem oraz wykonanie scenariuszy testowych (w ramach testów regresyjnych) dla funkcjonalności, na które poprawki mogły mieć wpływ.
- 4.3.2.7. Wykonawca po każdej turze testów przygotowuje raport z testów i przekaże go Zamawiającemu. Raport powinien zawierać zestawienie przeprowadzonych scenariuszy testowych, wyniki testów oraz zestawienie błędów Systemu Automatyzacji. Błędy muszą zostać usunięte przez Wykonawcę przed następną turą testów.
- 4.3.3. Procedura odbioru rozwiązania w zakresie dodatkowych algorytmów/zadań do zarządzania środowiskiem wirtualnym oraz zbiorczych algorytmów/zadań jako procedur uruchamiających zestaw pojedynczych algorytmów/zadań:
  - 4.3.3.1. Podstawą zgłoszenia do odbioru algorytmów zadań jest zrealizowanie prac przewidzianych w ramach budowy Systemu Automatyzacji.
- 4.3.4. Podstawą weryfikacji algorytmów zadań przekazanych do odbioru będą:
  - 4.3.4.1. Wykonanie testów akceptacyjnych określonych w poniższym planie testów akceptacyjnych.
  - 4.3.4.2. Testy akceptacyjne przeprowadza Wykonawca na środowisku wskazanym przez Zamawiającego. Nadzór nad testami akceptacyjnymi sprawuje Zamawiający. W Testach Akceptacyjnych uczestniczą przedstawiciele Zamawiającego i Wykonawcy.
  - 4.3.4.3. Testy akceptacyjne przeprowadzone zostaną w ramach maksymalnie trzech tur, trwających max. 5 dni roboczych dla każdej z tur, pomiędzy którymi Wykonawca będzie dokonywał wgrywania poprawek do błędów zgłoszonych w efekcie przeprowadzonych testów akceptacyjnych. Przerwa pomiędzy turami testów akceptacyjnych nie może być dłuższa niż 3 dni robocze.
  - 4.3.4.4. Pierwsza tura polegać będzie na przeprowadzeniu wszystkich uzgodnionych w planie testów akceptacyjnych scenariuszy testowych,

- 4.3.4.5. Druga tura odbędzie się, jeżeli podczas pierwszej tury zostały wykryte błędy. Obejmować będzie przeprowadzenie scenariuszy testowych, które w pierwszej turze zakończyły się niepowodzeniem oraz wykonanie scenariuszy testowych (w ramach testów regresyjnych) dla funkcjonalności, na które poprawki mogły mieć wpływ.
- 4.3.4.6. Trzecia tura odbędzie się, jeżeli podczas drugiej tury zostały wykryte błędy. Obejmować będzie przeprowadzenie scenariuszy testowych, które w drugiej turze zakończyły się niepowodzeniem oraz wykonanie scenariuszy testowych (w ramach testów regresyjnych) dla funkcjonalności, na które poprawki mogły mieć wpływ.
- 4.3.4.7. Wykonawca po każdej turze testów przygotowuje raport z testów i przekazuje go Zamawiającemu. Raport powinien zawierać zestawienie przeprowadzonych scenariuszy testowych, wyniki testów oraz zestawienie błędów. Błędy muszą zostać usunięte przez Wykonawcę przed następną turą testów.

## 5. Dokumentacja Systemu Automatyzacji

Wykonawca wykona i dostarczy Dokumentację Projektową w zakresie:

- Instalacji i konfiguracji Systemu w zakresie uwzględnienia przeprowadzenia czynności instalacji i końcowej konfiguracji Systemu jego komponentów. Zamawiający dopuszcza w uzgodnionych elementach odwołania do standardowej dokumentacji udostępnionej przez producenta oprogramowania.
- Instrukcji Administratora Systemu, zawierające informacje niezbędne do samodzielnego konfigurowania i administrowania Systemem.
- Instrukcji Użytkowników Systemu z uwzględnieniem ich roli w Systemie.
- Koncepcji Architektury Systemu zawierającej szczegółowy opis komponentów Systemu, interfejsów integracji.

Wykonawca zobowiązany jest do opracowania dokumentu oraz jego aktualizacji na skutek ustaleń w trakcie Wdrożenia i uruchomienia produkcyjnego Systemu, tj. przygotowanie dokumentu w ramach Dokumentacji Powykonawczej.

- Dokumentacja przygotowana i przekazana do odbiorów w wersji pdf oraz w wersji edytowalnej w MS Word lub MS Excel.

- Dokumentacja Projektowa musi zostać przygotowana w języku polskim z możliwością wykorzystania anglojęzycznych nazw własnych komponentów informatycznych.

## 6. Analiza Ryzyka

Wykonawca zobowiązuje się, że w ciągu 35 dni od dnia wdrożenia Oprogramowania i konfiguracji wymienionych w ust.3, przeprowadzi Analizę Ryzyka Bezpieczeństwa Informacji. Analiza musi być zgodna z metodyką PN/ISO-IEC 27005, bazująca na normie PN-ISO/IEC 27001 oraz RODO, w szczególności: identyfikację ryzyka w zakresie dostarczonego oprogramowania oraz przeprowadzi klasyfikację ryzyka wraz z szacowaniem ryzyka umożliwiającym obniżenie ryzyka do poziomu akceptowalnego przez Zamawiającego. Wykonawca zobowiązany jest do opracowania dokumentu oraz aktualizacji dokumentu w trakcie wdrażania oprogramowania i przekazania go do Zamawiającego. Wykonawca zobowiązany jest do wprowadzenia zidentyfikowanych zabezpieczeń na środowiskach wykorzystywanych podczas Wdrożenia.