

## ZAŁĄCZNIK NR 2.01 DO UMOWY

# PROCEDURA TESTOWANIA

w postępowaniu pn.:

**Dostawa wraz z montażem, uruchomieniem, konfiguracją i testami aktywnych urządzeń sieciowych w projekcie „Pomorskie e-Zdrowie”**

## 1. Procedura Testowa.

1. Procedura dotyczy testów funkcjonalnych Komponentów poprzedzających Odbiór komponentu, zgodnie z Harmonogramem wdrożenia.
2. Termin i czas przeprowadzenia poszczególnych testów funkcjonalnych zostanie określony w Harmonogramie wdrożenia.
3. Przygotowanie testów funkcjonalnych:
  - a. Wykonawca w terminie uzgodnionym z Zamawiającym dla poszczególnych testów funkcjonalnych prześle do akceptacji Zamawiającemu plan i zakres testów. i) Plan testów musi zawierać co najmniej:
    - i. proponowany czas trwania testu wraz z iteracjami, o których mowa w pkt 6),
    - ii. podstawowe informacje na temat przedmiotu testów,
    - iii. nazwę Komponentu, nazwę modułu, nazwę funkcjonalności,
    - iv. scenariusz testów danej funkcjonalności, wraz z informacją o konfiguracji (jeżeli jest wymagana dodatkowa), kryteria akceptacyjne.
  - b. Zamawiający wniesie ewentualne uwagi do przedstawionego planu testu w ciągu 7 dni roboczych.
  - c. Wykonawca uwzględni uwagi Zamawiającego oraz prześle poprawiony plan testów w ciągu 3 dni roboczych.
  - d. Brak akceptacji planu testu uniemożliwia rozpoczęcie testów funkcjonalnych danego Komponentu.
4. Zakres testów funkcjonalnych, będzie odpowiadał zakresowi realizacji danego Komponentu w ramach danego etapu i będzie obejmować kompletność, poprawność instalacji i działania Przedmiotu Zamówienia w zakresie określonym w rozdziale 2.
5. Przed przystąpieniem do testów funkcjonalnych Wykonawca jest zobowiązany przedstawić Dokumentację użytkową zgodną z wersją testowanego Komponentu.
6. Iteracje testów i reakcja na Wady w trakcie wykonywania testów funkcjonalnych:
  - a. Pierwsza iteracja testów:
    - i. w trakcie testów Zamawiający na bieżąco zgłasza Wady.
    - ii. po zakończeniu realizacji testów, Wykonawca prześle Zamawiającemu protokół rozbieżności, zawierający Wady.
    - iii. czas usunięcia wszystkich Wad po pierwszej iteracji: do 5 dni roboczych od przekazania protokołu rozbieżności.
  - b. Druga iteracja testów - weryfikacja usuniętych Wad zgłoszonych w pierwszej iteracji testów:
    - i. w trakcie testów Zamawiający na bieżąco zgłasza Wady.
    - ii. po zakończeniu realizacji testów, Wykonawca prześle Zamawiającemu protokół rozbieżności, zawierający Wady.
    - iii. czas usunięcia wszystkich Wad po drugiej iteracji: do 3 dni roboczych od przekazania protokołu rozbieżności.
  - c. Trzecia iteracja testów - weryfikacja usuniętych Wad zgłoszonych w poprzednich iteracjach testów:

- i. w trakcie testów Zamawiający na bieżąco zgłasza Wady.
    - ii. po zakończeniu realizacji całego scenariusza testowego, Wykonawca przekazuje Zamawiającemu protokół rozbieżności, zawierający Wady.
    - iii. czas usunięcia wszystkich Wad po trzeciej iteracji: do 2 dni roboczych od przekazania protokołu rozbieżności.
  - d. Czwarta iteracja testów - weryfikacja usuniętych Wad zgłoszonych w poprzednich iteracjach testów.
7. W sytuacji, gdy pomimo dokonania iteracji testów wskazanych w pkt 6), testy nie zakończą się pomyślnie, a Wady są istotne – uniemożliwiające prawidłowe korzystanie z Przedmiotu Zamówienia Zamawiający może odstąpić od realizacji Umowy z przyczyn leżących po stronie Wykonawcy.
8. Zakończenie testów funkcjonalnych z wynikiem pozytywnym umożliwia Odbiór Komponentu, etapu, końcowy zgodnie z „Procedurą odbiorową” stanowiącą załącznik nr 2.02 do Umowy.
9. Wszelkie powiadomienia przez Strony, w trakcie testów funkcjonalnych, odbywać się będą w formie pisemnej z wykorzystaniem poczty elektronicznej w ramach ustalonego w Dokumentacji Analizy przedwdrożeniowej kanału komunikacyjnego.
10. Testy funkcjonalne Komponentu zakończą się Raportem z testów funkcjonalnych, który musi być przyjęty przez Zamawiającego bez zastrzeżeń.

## 2. Minimalny zakres Testów funkcjonalnych

### 1. Sieć LAN

- 1.1. Sprawdzenie konfiguracji sprzętowej urządzenia i wersji oprogramowania.
- 1.2. Sprawdzenie możliwości zalogowania się do urządzenia i zdalnej konfiguracji z wybranej stacji administracyjnej.
- 1.3. Przetestowanie mechanizmów niezawodnościowych przełączników poprzez symulację awarii elementów redundantnych (zasilaczy, modułów zarządzania, stacka)
- 1.4. Symulacja wystąpienia pętli w sieci LAN na poziomie pojedynczego przełącznika oraz całej sieci LAN.
- 1.5. Redundancja połączeń – symulacja awarii fizycznej i logicznej (jeśli możliwe).
- 1.6. Sprawdzenie łączności w wybranej sieci VLAN.
- 1.7. Sprawdzenie łączności do Internetu z wybranego VLAN.
- 1.8. Weryfikacja polityk dla Firewall
- 1.9. Weryfikacja działania antywirusa skanowania spakowanych plików, kwarantanny w email dla Firewall,
- 1.10. Weryfikacja transparentnej integracji z AD (jeśli zrealizowana)
- 1.11. Testy wydajności Firewall
- 1.12. Weryfikacja powiadamiania odnośnie zdarzeń

### 2. Sieć WLAN

- 2.1. Przetestowanie mechanizmów niezawodnościowych rozwiązania WLAN poprzez symulację awarii bezprzewodowych punktów dostępowych

- 2.2. Zalogowanie się do sieci WLAN w trybie gość poprzez Portal logowania.
- 2.3. Zalogowanie się do sieci WLAN jako pracownik.
- 2.4. Weryfikacja mechanizmów roamingu.
3. Oprogramowanie Zarządzające
  - 3.1. Sprawdzenie podłączenia do systemu wszystkich wymaganych urządzeń
  - 3.2. Sprawdzenie poprawności instalacji
  - 3.3. Sprawdzenie poprawności dostarczanych do rozwiązania licencji
  - 3.4. Sprawdzenie uprawnień dla poszczególnych użytkowników
  - 3.5. Sprawdzenie poprawności działania alertów
  - 3.6. Sprawdzenie poprawności działania raportów
  - 3.7. Sprawdzenie poprawności implementacji mapki
  - 3.8. Sprawdzenie poprawności wykonania i odtworzenia backupu konfiguracji urządzeń
  - 3.9. Sprawdzenie możliwości zarządzania urządzeniami poprzez rozwiązanie.
4. Bezpieczeństwo
  - 4.1. Sprawdzenie czy możliwy jest dostęp do sieci poprzez podłączenie się do niezajętego portu urządzenia.
  - 4.2. Sprawdzenie czy możliwy jest dostęp do konsoli urządzenia oraz przez zdalną sesję poprzez nieautoryzowanego administratora.
  - 4.3. Weryfikacja skonfigurowanych reguł komunikacji pomiędzy segmentami w sieci.