**Załącznik nr 4 do Umowy nr …………………..**

**Środowisko programowo-sprzętowe i wymagania techniczne**

# Środowisko programowo-sprzętowe

System składa się z następujących komponentów programowych:

Platforma Moodle:

1. Platforma e-learningowa Moodle (aktualnie w wersji oprogramowania Moodle 4.0.1
2. Serwer bazodanowy - MariaDB 10.3.38
3. System operacyjny - Debian 10

Każdy komponent funkcjonuje w ramach maszyny wirtualnej (VM) w ramach środowiska VMWare vSphere 8.0.

System składa się z następujących komponentów sprzętowych:

Maszyny wirtualne posiadają następujące parametry:

1. pamięć operacyjna: 4GB RAM z możliwością zwiększenia w razie potrzeby;
2. procesor: 2 x VCPU (2 rdzenie);
3. karta graficzna: 4 MB (brak akceleracji 3D);
4. kontroler SCSI: 1 x LSI Logic SAS;
5. dysk Twardy: 1 x 80 GB typu Thin z możliwością powiększenie w razie potrzeby;
6. 1 x napęd CD/DVD;
7. 1 x karta sieciowa vmxnet3;
8. zainstalowane oprogramowanie VMWare Tools.

# Wymagania techniczne

Zleceniobiorca zapewni prawidłowe wyświetlanie i funkcjonowanie Platformy w przeglądarkach internetowych (Microsoft Edge, Firefox, Opera, Safari, Chrome), zgodnych z ich najnowszymi

(aktualnymi na dzień zawarcia Umowy) wersjami oraz zapewni prawidłowe wyświetlanie i funkcjonowanie Platform w przeglądarkach internetowych zgodnie z najnowszymi wersjami, które pojawiły się w trakcie trwania Umowy.

Kod źródłowy musi być zgodny z rekomendacją W3C HTML 5 oraz przejść pozytywnie weryfikację przy pomocy narzędzi udostępnianych przez W3C pod adresami: [http://validator.w3.org](http://validator.w3.org/) i [http://jigsaw.w3.org/css-validator/.](http://jigsaw.w3.org/css-validator/)

Platforma Moodle oraz Produkty muszą być zgodne z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), w tym z załącznikiem nr 4 ww. rozporządzenia dotyczącym wymagań Web Content Accessibility Guidelines (WCAG 2.0).

Platforma posiada wbudowane zabezpieczenia, w tym:

1. odporność na ataki typu Brute Force; ochronę przed próbami nieautoryzowanego dostępu do panelu administracyjnego i kont użytkowników;
2. odporność na próby uzyskania dostępu poprzez znane formy włamań;
3. odporność na zmiany treści za pomocą specjalnych skryptów i manipulacji:
   1. ataki semantyczne na adres URL,
   2. ataki związane z ładowaniem plików,
   3. ataki typu cross-site scripting,
   4. ataki typu CSRF,
   5. podrabianie zatwierdzenia formularza,
   6. sfałszowanie żądania HTTP,
   7. ujawnienie uwierzytelnień dostępu,
   8. wstrzykiwanie kodu SQL,
   9. ujawnienie danych przechowywanych w bazie,
   10. kradzież cookies,
   11. przechwytywanie sesji,
   12. wstrzykiwanie sesji,
   13. zafiksowanie sesji,
   14. trawersowanie katalogów,
   15. wstrzykiwanie poleceń systemowych,
   16. ujawnianie kodu źródłowego np. plików .inc, „template” itp.