# Lista Dobrych Praktyk w Zakresie Utrzymania Bezpieczeństwa Sieciowego

**Administrator to osoba lub podmiot wyznaczony przez Zamawiającego, odpowiedzialny za zarządzanie, konfigurację, utrzymanie oraz bezpieczeństwo systemu, w tym nadawanie uprawnień użytkownikom, monitorowanie działania i zapewnienie zgodności z ogólnie przyjętymi zasadami i standardami.**

## 1. Dostęp do serwera

- Każdy administrator powinien posiadać indywidualne konto - dotyczy administratora/informatyka klienta oraz pracowników Wsparcia Vector Software Group.
- Na serwerze bazodanowym nie należy zakładać kont użytkowników nie administracyjnych.
- Aktywna praca w aplikacjach na serwerze bazodanowym jest niedozwolona.
- Jeśli wymagany jest dostęp przez Pulpit zdalny dla pracowników, należy wdrożyć dodatkową instancję serwera dedykowaną do takich połączeń wraz z odpowiednimi licencjami i zabezpieczeniami.

## 2. Porty i komunikacja

- Lista wymaganych portów:
- **Port 1434** – dla aplikacji korzystających z tej bazy danych (na serwerze)
- **Porty 80 i 443 (HTTP/HTTPS)** – dla stron internetowych, w tym systemów rezerwacji i operatorów płatności (na routerze przekierowane na serwer)
- Każde otwarcie innego portu powinno być dokładnie przemyślane i wdrożone z odpowiednimi mechanizmami ochrony, np. zaporą sieciową.

## 3. Połączenia spoza sieci wewnętrznej

- Zalecane narzędzie: **TeamViewer** – bezpieczne i uniwersalne rozwiązanie do realizacji zgłoszeń serwisowych przez Wsparcie Vector Software.
- Alternatywa: **Pulpit zdalny** – dozwolony wyłącznie przy połączeniach realizowanych poprzez VPN.

## 4. Sprzęt sieciowy

- **Przykładowa konfiguracja routera**:
- Porty: minimum 5 x Gigabit Ethernet oraz WAN 1 Gb
- Wydajność: do 1 Gbps z włączonymi funkcjami zabezpieczeń.
- Funkcje: wsparcie dla VPN, zaawansowana zapora sieciowa, VLAN

- **Konfiguracja** powinna obejmować:
- **Zmianę domyślnych danych logowania** – ustawienie silnego hasła administratora.
- **Włączenie zapory sieciowej (Firewall)** – w celu blokowania nieautoryzowanego ruchu.
- **Segmentację sieci** – podział na sieci VLAN dla różnych grup urządzeń.
- **Filtrowanie adresów IP** – ograniczenie dostępu do określonych adresów IP lub zakresów.
- **Ustawienie VPN** – skonfigurowanie usługi VPN do bezpiecznego dostępu zdalnego.
- **Regularne aktualizacje firmware** – w celu załatania znanych luk bezpieczeństwa.

**5. Antywirus**

- Na serwerach i urządzeniach klienckich należy zainstalować oprogramowanie antywirusowe.
- Przykład: **ESET Endpoint Security** – zaawansowane rozwiązanie oferujące ochronę przed wirusami, ransomware i innymi zagrożeniami.
- Regularne aktualizacje baz wirusów oraz skanowanie systemu przeprowadzane przez Administratora powinny być priorytetem.
- Zalecamy dodatkową licencję na zarządzanie zbiorcze instalacjami Eset na wszystkich stanowiskach

**6. Aktualizacje systemu**

- System operacyjny oraz zainstalowane oprogramowanie powinny być regularnie aktualizowane przy wsparciu administratora po stronie klienta

**7. Audyty bezpieczeństwa**

- Audyty pozwalają na identyfikację potencjalnych luk w zabezpieczeniach i ich szybkie usunięcie.

**8. Konto administratora**

- Konto administratora powinno być używane wyłącznie do celów zarządzania systemem.
- Nie zalecamy pracy na kontach niebędących kontami administracyjnymi (zwykły użytkownik) ze względu bezpieczeństwa. Ograniczenie codziennego dostępu oraz wykorzystanie kont o ograniczonych uprawnieniach w przypadku rutynowych działań poprawia bezpieczeństwo.
- Silne hasła oraz mechanizmy uwierzytelniania wieloskładnikowego (MFA) są obligatoryjne.

VECTOR SOFTWARE GROUP

# WYMAGANIA SPRZĘTOWE

**POS (Stanowisko kasowe)**

Minimum

- 4-rdzeniowy procesor IntelCeleron serii J1900 z taktowaniem min. 2.0 GHz lub podobny
- 6GB pamięci DDR3, preferowane 8GB
- dysk twardy o pojemności min. 120GB
- ekran 15" o rozdzielczości min. 1024x748 px

Zalecane

- procesor Intel i3-7100U z taktowaniem min 2.40 GHz lub podobny
- 8GB pamięci DDR3
- dysk twardy SSD o pojemności min. 120GB
- ekran 15-17" o rozdzielczości min 1280x1024 px

Optymalne

- procesor Intel i5-7200U z taktowaniem 3.10 GHz lub podobny
- 8GB pamięci DDR3, preferowane 16GB
- dysk twardy SSD o pojemności min. 120GB
- ekran 15-17" o rozdzielczości min. 1280x1024 px

System operacyjny Windows 11 wersja Professional

**DESKTOP (Stanowisko kasowe)**

Minimum

- procesor Intel Core i3-3240 z taktowaniem min 2.40 GHz lub podobny
- 8GB pamięci DDR3
- dysk twardy SSD o pojemności min. 120GB
- ekran 21" lub większy o rozdzielczości min. 1280x1024 px

Zalecane

- procesor Intel i5-7200U z taktowaniem 3.10 GHz lub podobny

- 16GB pamięci DDR3
- dysk twardy SSD o pojemności min. 120GB
- ekran 21" lub większy o rozdzielczości min. 1280x1024 px

System operacyjny Windows 11 wersja Professional

**SERWER**

Minimum

- procesor Intel minimum 4 rdzenie lub analogicznej wydajności.
- pamięć 16GB DDR4
- dysk twardy SSD o pojemności min. 480GB x 2 (RAID1)
- kontroler pamięci masowej RAID – np. PERC H355
- system operacyjny Windows Server 2022 Essential
- silnik bazy danych Microsoft SQL Server 2019 Express lub nowszy

Zalecane

- procesor Intel Xeon E-2334 3.4GHz 8MB cache (4 cores 8 threads) lub analogicznej wydajności
- pamięć 32GB DDR4 lub więcej
- dysk twardy SSD o pojemności min. 480GB x 2 (RAID 1)
- kontroler pamięci masowej RAID – np. PERC H355
- system operacyjny Windows Server 2022 Essential lub Standard
- silnik bazy danych Microsoft SQL Server 2022 Express lub Standard

Większe wymagania sprzętowe wynikają z wielozadaniowości takich jednostek - są wykorzystywane m.in do zarządzania oraz rozliczania sprzedaży (definiowanie wydarzeń/biletów, generowania raportów) czy zewnętrznych aplikacji np. programy biurowe i księgowe, przeglądarki internetowe.

**DRUKARKI FISKALNE**

Zalecane

- Novitus HD II Online (wariant z wyświetlaczem zintegrowanym lub wolnostojącym)
- Novitus Deon Online

**DRUKARKI BILETOWE (termiczne)**

Zalecane

- Boca L
- Bixolon XD5-40d lub XD3-40dK

**TERMINALE PŁATNICZE**

Do integracji modułu Kasa z terminalami płatniczymi wymagane jest urządzenie **Ingenico Lane 3000 lub Ingenico Lane 5000** dostarczony przez firmę eService lub Fiserv.

**Operatorzy płatności:**

- Tpay.com (https://tpay.com/)
- Przelewy24 (https://www.przelewy24.pl/)
- eService (https://www.eservice.pl/platnosci-internetowe)
- Dotpay (jeśli Nabywca posiada stare konto przed migracją do systemu Przelewy24)

**Opcje backupu bazy danych:**

- Backup zewnętrzny – ochrona przed uszkodzeniem plików bazodanowych.