



Kraków dnia 20 lutego 2025

NIP : 676-20-96-303

REGON : 000298554

KRS : 0000005002

Adres :  
ul. dr. Józefa Babińskiego 29  
30-393 Kraków  
tel. +48 12 652 43 47  
fax: +48 12 262 13 35  
e-mail: biuro@babinski.pl

## Zapytanie ofertowe

Szpital Kliniczny im. dr. J. Babińskiego SP ZOZ w Krakowie zaprasza do udziału w postępowaniu o udzielenie zamówienia w trybie do 130 000 zł netto i złożenia oferty cenowej.

Postępowanie dotyczy złożenia oferty cenowej dla zadania : przygotowanie, wdrożenie i uruchomienie dodatkowych zabezpieczeń serwerów DNS, stron WWW, poczty elektronicznej oraz głównego łącza.

### Opis przedmiotu zamówienia:

#### Etap I

1. Pomiary środowiska wirtualizacji:
  - 1.1. pomiary pamięci masowej,
  - 1.2. dobranie odpowiedniej konfiguracji systemu plików,
2. Rekonfigurowanie systemu operacyjnego pod nową pocztę:
  - 2.1. Debian GNU/Linux Bookworm (stable),
  - 2.2. Postfix (SMTP),
  - 2.3. Dovecot (IMAP/POP3),
  - 2.4. integracja systemu Postfix z Dovecot za pomocą protokołu LMTP,
  - 2.5. filtr SPAM (offline),
  - 2.6. filtr spamu czasu rzeczywistego,
  - 2.7. filtr antywirusowy (ClamAV),
  - 2.8. WebGUI (Roundcube i/lub Nextcloud),
3. Przygotowanie systemu operacyjnego pod nowe zabezpieczenia serwerów DNS:
  - 3.1. Debian GNU/Linux Bookworm (stable),
  - 3.2. Bind lub Dnsmasq.
  - 3.3. konfiguracja serwera DNS:
    - 3.3.1. MX,
    - 3.3.2. DMARC,
    - 3.3.3. SPF,
    - 3.3.4. DKIM.
4. Konfiguracja eksporterów krytycznych metryk systemowych oraz usługowych.
5. Konfiguracja zapory sieciowej w systemach operacyjnych.

#### Etap II

1. Przygotowanie środowiska testowego:
  - 1.1. testowa, wewnętrzna domena,
  - 1.2. konfiguracja systemu DNS na potrzeby środowiska testowego,
  - 1.3. opracowanie metody synchronizacji danych ze środowiskiem produkcyjnym.
2. Wdrożenie zaawansowany system monitoringu oparty o stos Grafana, Loki, Prometheus:
  - 2.1. szczegółowe monitorowanie parametrów pracy maszyny wirtualnej,
  - 2.2. zbieranie logów z krytycznych podsystemów infrastruktury pocztowej,



- 2.3. konfiguracja wizualizacji,
- 2.4. brak limitów (użytkowników, aplikacji),
- 2.5. Brak opłat licencyjnych.

### Etap III

- 1. Migracja kont pocztowych oraz wiadomości email do zbudowanego systemem MFA:
  - 1.1. przygotowanie dedykowanego oprogramowania do automatycznej migracji skrzynek pocztowych i użytkowników
    - 1.1.1. minimalne wymagania:
      - 1.1.1.1. mapowanie lokalnych użytkowników na konta domenowe AD
      - 1.1.1.2. mapowanie aliasów pocztowych na konta pocztowe
      - 1.1.1.3. mapowanie ograniczeń przestrzeni dyskowej dla kont pocztowych
- 2. Konfiguracja serwera http reverse proxy + TLS Termination,
- 3. Opracowanie systemu informacji o urlopach:
  - 3.1. możliwość włączania opcji automatycznego odpowiadania na wiadomości w okresie urlopowym,
  - 3.2. możliwość samodzielnego definiowania okresów urlopowych przez użytkowników poczty,
  - 3.3. możliwość ustawienia treści automatycznie generowanej wiadomości,
- 4. Testy działania,
- 5. Pomiary wydajności systemu,
- 6. Ostateczne poprawki,

### Etap IV

- 1. Przełączenie na nowy system pocztowy,
- 2. Uruchomienie przygotowanych zabezpieczeń,
- 3. Poprawki konfiguracji,
- 4. Szkolenia

### Szkolenia dla administratorów

- 1. Ścieżki exploitacji systemów GNU/Linux,
  - 2. Mechanizmy monitorowania i ochrony jądra Linux,
  - 3. Dokładne wprowadzenie do dostępnych narzędzi i ich możliwości (np. auditd, eBPF),
  - 4. Częste błędy konfiguracji,
  - 5. Omówienie protokołu TLS jako podstawy do nawiązywania bezpiecznych, zaszyfrowanych połączeń
  - 6. Zapewnianie bezpiecznego dostępu zdalnego do serwera – SSH
    - 6.1. podstawowa konfiguracja
    - 6.2. zabezpieczenia serwera SSH
    - 6.3. strategie zarządzania konfiguracją po stronie klienta
  - 7. Konteneryzacja (Docker, Podman),
  - 8. Serwery HTTP/HTTPS,
  - 9. Współdzielenie plików,
  - 10. Szyfrowanie lokalne (GPG, LUKS).
  - 11. Omówienie protokołu SMTP na podstawie oprogramowania Postfix:
    - 11.1. rola protokołu SMTP w dostarczaniu wiadomości,
-



- 
- 
- 11.2. omówienie procesu wysyłania wiadomości od momentu kliknięcia „wyślij” do momentu dostarczenia wiadomości do skrzynki docelowej,
  - 11.3. techniki radzenia sobie ze spamem i niechcianymi wiadomościami,
  - 11.4. komunikacja szyfrowana,
  - 11.5. mechanizmy służące do zabezpieczania serwerów SMTP: SPF, DKIM, DMARC.
12. Omówienie protokołu IMAP na podstawie oprogramowania Dovecot:
- 12.1. rola protokołu IMAP w ekosystemie pocztowym,
  - 12.2. omówienie najważniejszych komend związanych z protokołem IMAP,
  - 12.3. techniki zabezpieczania dostępu do serwerów IMAP,

### Wymagania dotyczące wsparcia technicznego

- 1. Minimum rok wsparcia technicznego, które obejmuje:
- 2. ◦ pomoc w rozwiązywaniu problemów technicznych i awarii systemu pocztowego,
- 3. ◦ rekonfiguracja systemu pocztowego, w tym:
- 4. ▪ możliwość dodania nowej domeny,
- 5. ▪ rekonfiguracja zabezpieczeń serwera smtp:
  - 5.1. konfiguracja ograniczeń dla klientów, komendy helo/ehlo, wysyłających, odbiorców i przekazywania poczty,
  - 5.2. dostrajanie filtrów SPAMu,
  - 5.3. konfiguracja dynamicznych list RBL, whitelist dla serwerów SMTP,
  - 5.4. konfiguracja statycznych whitelist, blacklist dla serwerów SMTP.

Oferty należy składać na platformie zakupowej.

Termin składania ofert upływa 28 luty 2025r. o godzinie 10:00.

podpis Dyrektora Szpitala

---

---