

## SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. **PRZEDMIOTEM ZAMÓWIENIA** jest świadczenie usług informatycznych w Okręgowym Szpitalu Kolejowym w Katowicach, polegających na bieżącej obsłudze istniejącej infrastruktury IT.
2. **SŁOWNIK POJĘĆ:**
  - 2.1. **Gotowość serwisowa** – dyżur telefoniczny oraz gotowość do podjęcia działań na wykryte lub zgłoszone awarie, usterki, błędy;
  - 2.2. **Oprogramowanie** - ogół informacji w postaci zestawu instrukcji, zaimplementowanych interfejsów i zintegrowanych danych przeznaczonych dla komputera do realizacji wyznaczonych celów;
  - 2.3. **Infrastruktura Sprzętowa** - fizyczne komponenty stanowiące rdzeń infrastruktury IT w szpitalu. Należą do nich serwery, komputery, sieć i sprzęt peryferyjny;
  - 2.4. **Awaria** - kategoria wady w Oprogramowaniu lub Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie ponad połowy Infrastruktury lub brak możliwości pracy w kluczowych systemach Szpitala;
  - 2.5. **Usterka** - kategoria wady w Oprogramowaniu lub Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie mniej niż połowy Infrastruktury;
  - 2.6. **Błąd** - kategoria wady w Oprogramowaniu lub Infrastrukturze oznaczającą funkcjonowanie niezgodne z oczekiwaniem (przeznaczeniem), która nie wpływa istotnie na funkcjonowanie całej Infrastruktury;
  - 2.7. **Incydent Bezpieczeństwa Informacji (Incydent)** - Pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji;
  - 2.8. **Czas pracy** - od poniedziałku do piątku, w godzinach od 7:00-17:00 z wyłączeniem dni wolnych od pracy;
  - 2.9. **Dni wolne od pracy** – dni ustawowo wolne od pracy oraz święta;
  - 2.10. **Okno serwisowe** – czas, w którym Wykonawca wykonuje prace serwisowe, tj.: aktualizacje systemów, których nie można aktualizować w Czasie pracy. Okno serwisowe obejmuje czas od poniedziałku do piątku, w godzinach od 17:00- 6:00 z wyłączeniem dni wolnych od pracy. W przypadkach, gdy konieczne jest wykonanie prac serwisowych w dni wolne od pracy, prace te mogą być realizowane poza standardowym oknem serwisowym po uprzednim uzgodnieniu ich zakresu, terminu oraz zatwierdzeniu proponowanych godzin realizacji przez Zamawiającego.
  - 2.11. **Pogotowie awaryjne** – dyżur telefoniczny 24/7 obsługujący Awarie, zgodnie z terminami:
    - przyjmowanie zgłoszeń: natychmiast
    - podjęcie działań w celu usunięcia awarii: do 2 godzin
    - gwarantowane przywrócenie systemów do działania: do 8 godzin
  - 2.12. **SOC** - usługa monitoringu aktywnego realizowana 24/7, polegająca na monitorowaniu zdarzeń naruszenia cyberbezpieczeństwa, analiza oraz zarządzanie incydentami bezpieczeństwa;
3. **USŁUGI BĘDĄ REALIZOWANE W NASTĘPUJĄCYCH FORMACH:**
  - **serwis lokalny** – usługi świadczone w szpitalu lub w lokalizacjach wskazanych przez Zamawiającego – do oceny wykonawcy, zgodnie z potrzebami w celu realizacji usługi;
  - **serwis zdalny** – usługi realizowane za pomocą dedykowanego oprogramowania do pracy

zdalnej z wykorzystaniem bezpiecznego i szyfrowanego połączenia internetowego, zgodnie z procedurami ustalonymi przez Strony;

- **serwis poprzez kanał VPN** – usługi świadczone z wykorzystaniem bezpiecznego i szyfrowanego połączenia VPN z siecią szpitala.

#### 4. OGÓLNE ZASADY REALIZACJI USŁUGI:

- 4.1. Zamawiający wymaga, by Wykonawca zapewnił **minimum 90 godzin roboczych pracy informatyków** w miesiącu (w powyższą ilość godzin nie jest wliczona usługa monitoringu aktywnego 24/7), a w przypadku, w którym do osiągnięcia założeń opisanych w niniejszym dokumencie i SWZ będzie konieczne wykonanie większej liczby godzin, niż przewidziano, godziny te zostaną wliczone w ustalone miesięczne wynagrodzenie (ryczałt) i nie będą stanowiły podstawy do odrębnego rozliczenia.
- 4.2. Godziny świadczenia usługi: dni robocze w godzinach od 7:00 do 17:00 oraz możliwość zgłoszenia awarii poza godzinami pracy serwisu.
- 4.3. **Zakres sprzętu do obsługi:** Serwery wirtualizacji, macierz dyskowa, infrastruktura sieciowa, ok. 160 komputerów stacjonarnych. Zamawiający z uwagi na stosowane polityki bezpieczeństwa nie wskazuje dokładnie rodzaju sprzętu oraz stosowanych środowisk informatycznych i sieciowych, natomiast umożliwia przeprowadzenie wizji lokalnej opisanej w ust. 3.5 SWZ.
- 4.4. W ramach świadczenia przedmiotowej usługi Wykonawca będzie identyfikował potrzeby i zagrożenia w obszarze bezpieczeństwa IT, a następnie rekomendował Zamawiającemu konkretne rozwiązania technologiczne (w tym sprzętowe i programowe), które należy zakupić w celu zwiększenia poziomu cyberbezpieczeństwa.
- 4.5. W ramach świadczenia przedmiotowej usługi Wykonawca musi zapewnić **sprzęt zastępczy** w zakresie krytycznych dla Zamawiającego obszarów działania (serwery, urządzenia sieciowe, macierz dyskowa) w celu umożliwienia ciągłości działania systemów informatycznych szpitala. Zapewnienie sprzętu zastępczego w pozostałych obszarach stanowi kryterium punktowane i nie jest wymagane przez Zamawiającego.
- 4.6. Wykonawca posiada wdrożony System Zarządzania Ciągłością Działania zgodnie z normą ISO 22301 potwierdzony certyfikatem wydanym przez akredytowaną jednostkę certyfikującą oraz zobowiązuje się do utrzymywania i stosowania tego systemu zgodnie z wymaganiami tej normy przez cały okres obowiązywania umowy ws. zamówienia.
- 4.7. Wykonawca posiada wdrożony System Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001 potwierdzony certyfikatem wydanym przez akredytowaną jednostkę certyfikującą oraz zobowiązuje się do utrzymywania i stosowania tego systemu zgodnie z wymaganiami tej normy przez cały okres obowiązywania umowy ws. zamówienia.
- 4.8. Wykonawca wdrożył i stosuje zintegrowany system zarządzania jakością i zarządzania środowiskiem zgodnie z normą PN-EN ISO 9001:2015 oraz zobowiązuje się do utrzymywania i stosowania tego systemu zgodnie z wymaganiami tej normy przez cały okres obowiązywania umowy ws. zamówienia.

#### 5. GWARANTOWANE CZASY PRZYJMOWANIA ZGŁOSZEŃ, REAKCJI NA ZGŁOSZENIA ORAZ PRZYWRÓCENIA DO PEŁNEGO DZIAŁANIA:

##### 5.1. Gotowość serwisowa dla Awarii:

- Przyjmowanie zgłoszeń telefoniczne lub poprzez helpdesk: natychmiast
- Podjęcie działań w celu usunięcia awarii: do 2 godzin
- Gwarantowane przywrócenie systemów do działania: do 8 godzin

##### 5.2. Gotowość serwisowa dla Usterki:

- Przyjmowanie zgłoszeń telefoniczne lub poprzez helpdesk: natychmiast
- Podjęcie działań w celu usunięcia usterki: do 6 godzin
- Gwarantowane przywrócenie systemów do działania: do 24 godzin

##### 5.3. Gotowość serwisowa dla Błędu:

- Przyjmowanie zgłoszeń telefoniczne lub poprzez helpdesk: natychmiast
- Podjęcie działań w celu usunięcia błędu: do 16 godzin
- Gwarantowane usunięcie błędu: do 48 godzin

## **6. ZASADY REALIZACJI MONITORINGU AKTYWNEGO (SOC):**

- 6.1. Zamawiający wymaga wyznaczenia do realizacji SOC osobnego zespołu składającego się z minimum 12 osób, w którego skład wchodzi osoby o wskazanych poniżej rolach i z uwzględnieniem podzielonej odpowiedzialności za poszczególne zadania, co jest konieczne dla zapewnienia prawidłowej realizacji usługi:
- operatorzy I linii wsparcia – **co najmniej 4 osoby**
  - operator II linii wsparcia – **co najmniej 2 osoby**
  - operator III linii wsparcia – **co najmniej 1 osoba**
  - SOC manager – **co najmniej 1 osoba**
  - ekspert od zarządzania podatnościami – **co najmniej 1 osoba**
  - ekspert od bezpieczeństwa urządzeń – **co najmniej 1 osoba**
  - ekspert od ochrony danych osobowych – **co najmniej 1 osoba**
  - ekspert od zgodności z NIS2 i KSC – **co najmniej 1 osoba**
- 6.2. Wszystkie osoby, o których mowa powyżej, powinny biegle posługiwać się językiem polskim (w mowie i piśmie), w przeciwnym wypadku Wykonawca musi zapewnić tłumacza zapewniającego stałe tłumaczenie dla potrzeb realizacji zamówienia.

## **7. SZCZEGÓŁOWY ZAKRES USŁUGI:**

### **7.1. Podstawowy zakres świadczonej usługi:**

- a) zapewnienie ciągłości działania infrastruktury krytycznej,
- b) aktualizacja i planowanie serwisów infrastruktury IT,
- c) tworzenie i wdrażanie planów awaryjnych oraz polityk bezpieczeństwa IT,
- d) zarządzanie środowiskiem poczty elektronicznej i uprawnieniami użytkowników,
- e) diagnozowanie i rozwiązywanie problemów krytycznej infrastruktury IT,
- f) tworzenie dokumentacji technicznej i instrukcji użytkowych,
- g) współpraca z producentami sprzętu i oprogramowania,
- h) rejestracja rozwiązań sprzętowych, sieciowych oraz uprawnień użytkowników,
- i) analiza trendów i przewidywanie przyszłych problemów,
- j) doradztwo w zakresie architektury systemów i aplikacji,
- k) wsparcie dla procesów skalowania infrastruktury IT,
- l) analiza potrzeb biznesowych i doradztwo technologiczne,
- m) konsultacje w zakresie najlepszych praktyk DevOps i bezpieczeństwa IT,
- n) optymalizacja procesów biznesowych za pomocą technologii IT,
- o) integracja systemów i aplikacji,
- p) zarządzanie zmianą w infrastrukturze IT i procesach operacyjnych,
- q) przeprowadzenie raz w roku testów penetracyjnych (testy zewnętrzne, wewnętrzne i aplikacyjne), opracowanie zaleceń,
- r) wspieranie pracowników sekcji IT w zabezpieczaniu systemów i infrastruktury,
- s) tworzenie polityk ciągłości działania oraz odzyskiwania po awariach,
- t) przeprowadzanie pełnej inwentaryzacji systemów oraz sprzętu w trakcie realizacji przedmiotu zamówienia.

### **7.2. Bieżąca obsługa, administracja klastrem urządzeń UTM Zamawiającego, a w szczególności:**

- a) regularne sprawdzanie aktualności baz sygnatur, wersji licencjonowanych modułów
- b) regularne sprawdzanie aktualności wersji oprogramowania wewnętrznego
- c) regularny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich
- d) przeprowadzanie zmian w konfiguracji ogólnej systemu - adresy IP, DNS, DHCP, routing,

**NTP**

- e) konfiguracja interfejsów sieciowych - WAN, LAN, DMZ wg potrzeb
  - f) konfiguracja, rekonfiguracja dodatkowego łącza zapasowego
  - g) audyt początkowy polityk skonfigurowanych na urządzeniach, optymalizacja używanych reguł, zgodnie z dobrymi praktykami,
  - h) tworzenie nowych polityk, aktualizacja istniejących wg potrzeb,
  - i) integracja klastra UTM z Active Directory, instalacja i konfiguracja Agenta FSSO oraz pobranie bazy użytkowników LDAP,
  - j) instalacja najnowszego oprogramowania wewnętrznego (tylko stabilne wersje oprogramowania), przy czym aktualizacje krytyczne będą instalowane niezwłocznie po ogłoszeniu przez producenta,
  - k) audyt reguł i ustawień, weryfikacja i poprawienie reguł oraz ustawień wg potrzeb i w zgodzie z dobrymi praktykami,
  - l) konfiguracja, monitoring loadbalancingu dla dwóch łączy WAN,
  - m) zmiany w konfiguracji QoS oraz kształtowania pasma dla istniejących profili,
  - n) optymalizacja istniejących obiektów sieciowych zgodnie z dobrymi praktykami,
  - o) optymalizacja istniejących reguł firewall oraz NAT zgodnie z dobrymi praktykami,
  - p) optymalizacja konfiguracji IPSec VPN zgodnie z dobrymi praktykami,
  - q) optymalizacja filtrów URL oraz SSL, konfiguracja inspekcji SSL zgodnie z dobrymi praktykami,
  - r) opracowanie i wdrożenie polityki deszyfracji danych szyfrowanych SSL (Secure Sockets Layer), opracowanie reguł działania w zależności od rodzaju ruchu, opracowanie polityki ponownego szyfrowania danych, konfiguracja urządzeń UTM,
  - s) konfiguracja przesyłania logów do posiadanych przez Szpital instancji zbierających i przechowujących logi,
  - t) optymalizacja podziału sieci LAN na podsieci (VLANy),
  - u) zakładanie zgłoszeń serwisowych u producenta w imieniu Szpitala,
  - v) realizacja procesu naprawy i wymiany w ramach gwarancji producenta (również za granicą),
- 7.3. Bieżąca obsługa, administracja urządzeniami sieci LAN oraz Wi-fi, a w szczególności:**
- a) aktualizacja oprogramowania układowego przełączników do najnowszej stabilnej wersji,
  - b) konfiguracja sieci wirtualnych przełącznika na podstawie obecnej infrastruktury,
  - c) konfiguracja agregacji połączeń do serwerów pomiędzy przełącznikami,
  - d) konfiguracja agregacji połączeń dla przełączników dostępowych,
  - e) konfiguracja syslog dla przełączników,
  - f) konfiguracja protokołu SNMP zgodnie z obecnym systemem monitoringu,
  - g) konfiguracja użytkowników administracyjnych przełącznika zgodnie z politykami bezpieczeństwa oraz z dobrymi praktykami,
  - h) konfiguracja autoryzacji użytkowników SSH oraz www w oparciu o serwer radius. Wykonawca zainstaluje i skonfiguruje serwery RADIUS (podstawowy oraz zapasowy) wobec których będzie następowała autoryzacja użytkowników przechowywanych w katalogu LDAP,
  - i) konfiguracja NTP – dla wszystkich przełączników należy skonfigurować synchronizację czasu w oparciu o serwery lokalne, konfiguracja strefy czasowej,
  - j) regularne wykonywanie kopii zapasowej bieżącej konfiguracji dla wszystkich urządzeń sieciowych,
  - k) konfiguracja protokołów CDP oraz LLDP,
  - l) konfiguracja protokołu STP na wszystkich urządzeniach sieciowych,
  - m) konfiguracja serwera DNS oraz domeny wyszukiwania na wszystkich urządzeniach sieciowych,
  - n) konfiguracja możliwych do wdrożenia dodatkowych zabezpieczeń,
  - o) instalacja, konfiguracja systemu klasy NAC, zabezpieczenie sieci LAN, WiFi przed nieautoryzowanym dostępem,



**7.4. Bieżąca obsługa, administracja posiadanymi serwerami, macierzami, systemami operacyjnymi, systemem wirtualizacji, a w szczególności:**

- a) aktualizacja oprogramowania do najnowszej stabilnej wersji, przy czym aktualizacje krytyczne będą instalowane niezwłocznie po ogłoszeniu przez producenta,
- b) instalacja najnowszego oprogramowania wewnętrznego urządzeń (tylko stabilne wersje oprogramowania), przy czym aktualizacje krytyczne będą instalowane niezwłocznie po ogłoszeniu przez producenta,
- c) utrzymanie zgodności systemów z wymaganiami prawnymi dotyczącymi cyberbezpieczeństwa,
- d) pomoc zdalną w rozwiązywaniu problemów z serwerami i oprogramowaniem serwerowym,
- e) monitorowanie dostępności serwerów i usług,
- f) reagowanie na problemy związane z dostępnością serwerów,
- g) zarządzanie zmianami i wersjami oprogramowania serwerowego,
- h) zarządzanie patchami i aktualizacjami oprogramowania,
- i) monitorowanie wydajności systemów i aplikacji,
- j) diagnozowanie i rozwiązywanie problemów z wydajnością,
- k) zarządzanie konfiguracją systemów i aplikacji,
- l) automatyzacja rutynowych zadań operacyjnych,
- m) audyt konfiguracji i zabezpieczeń systemów,
- n) zarządzanie użytkownikami i uprawnieniami,
- o) zarządzanie środowiskami deweloperskimi, testowymi i produkcyjnymi,
- p) wykonywanie migracji systemów i aplikacji wg potrzeb,
- q) przeglądy systemów pod kątem najlepszych praktyk i zaleceń,
- r) administracja, zarządzanie i konfiguracja systemów chmurowych,
- s) ocena wykorzystania zasobów IT, optymalizacja wykorzystania zasobów,

**7.5. Bieżąca obsługa, administracja systemem tworzenia kopii zapasowych, a w szczególności:**

- a) aktualizacja oprogramowania do najnowszej stabilnej wersji, przy czym aktualizacje krytyczne będą instalowane niezwłocznie po ogłoszeniu przez producenta,
- b) instalacja najnowszego oprogramowania wewnętrznego urządzeń (tylko stabilne wersje oprogramowania), przy czym aktualizacje krytyczne będą instalowane niezwłocznie po ogłoszeniu przez producenta,
- c) utrzymanie zgodności systemów z wymaganiami prawnymi dotyczącymi cyberbezpieczeństwa,
- d) konfiguracja systemu kopii bezpieczeństwa,
- e) skonfigurowanie przestrzeni dla kopii bezpieczeństwa na zasobach Szpitala,
- f) konfigurację miejsc przechowywania (macierz, NASy itp.),
- g) opracowanie polityki tworzenia kopii zapasowych, składowania oraz harmonogramów,
- h) konfiguracja zadań backupowych,
- i) konfiguracja zabezpieczeń wewnętrznych, w tym kopii ratunkowej (ang. disaster recovery) systemu kopii bezpieczeństwa,
- j) instalacja, konfiguracja dodatkowych maszyn wirtualnych klientów, jeśli są wymagane, w środowisku Szpitala,
- k) konfiguracja kopii zapasowych maszyn wirtualnych Szpitala dla min. 1 repozytorium lokalnego oraz do zasobu chmurowego udostępnionego przez Wykonawcę (min. 20 TB powierzchni)
- l) instalacja niezbędnych agentów dla środowiska bazodanowego Szpitala i konfiguracja kopii zapasowych baz danych,
- m) konfigurację automatycznej weryfikacji kopii bezpieczeństwa maszyn wirtualnych,
- n) konfigurację powiadomień i codziennych raportów,
- o) regularne monitorowanie wykonywanych kopii zapasowych,
- p) regularne przeprowadzanie testów odtworzeniowych kluczowych systemów Szpitala

zgodnie z przyjętą polityką backupową,

- q) modyfikacja harmonogramu oraz zadań backupowych wg potrzeb Szpitala,

**7.6. Bieżąca obsługa, administracja domeną, a w szczególności:**

- a) aktualizacja oprogramowania do najnowszej stabilnej wersji, przy czym aktualizacje krytyczne będą instalowane niezwłocznie po ogłoszeniu przez producenta,
- b) konfiguracja zapasowego kontrolera domeny,
- c) cykliczne przeprowadzanie audytu domeny w celu podniesienie efektywności pracy administratorów, zwiększenie bezpieczeństwa danych, dostosowania do zgodności z najlepszymi praktykami oraz wytycznymi Microsoft,
- d) audyt uprawnień użytkowników,
- e) zarządzanie kontami użytkowników,
- f) zarządzanie grupami w usługach AD DS,
- g) zarządzanie obiektami typu komputer w AD DS,
- h) wdrażanie i zarządzanie OU,
- i) wdrażanie i zarządzanie obiektami GPO (Group Policy Object),
- j) konfiguracja zakresu i przetwarzania obiektów GPO,
- k) rozwiązywanie problemów z GPO,
- l) wdrażanie szablonów administracyjnych,
- m) konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów,
- n) konfiguracja preferencji zasad grupowych,
- o) zabezpieczanie kontrolerów domeny,
- p) implementacja polityki dotyczącej haseł i blokad,
- q) inspekcja zasad uwierzytelniania,
- r) zarządzanie bazą danych AD DS.,
- s) wdrażanie urzędów certyfikacyjnych (Certification Authority - CA),
- t) administrowanie Cas,
- u) zarządzanie certyfikatami SSL/TLS,
- v) utrzymanie, monitorowanie i rozwiązywanie problemów dotyczących CAs,
- w) zarządzanie procesem wdrażania, odwoływania i odzyskiwania certyfikatów,
- x) tworzenie kopii zapasowej bazy AD,
- y) monitorowanie AD DS,

**7.7. Usługa SOC monitorowania zdarzeń naruszenia cyberbezpieczeństwa, analiza oraz zarządzanie incydentami bezpieczeństwa, a w szczególności:**

- a) instalacja, konfiguracja systemu SIEM/XDR z modułami NDR, EDR,
- b) konfiguracja przesyłania logów z systemów Szpitala do systemu SIEM: UTM, routery, Antywirus (EDR), Antyspam, kontrolery domeny AD, przełączniki sieciowe, punkty dostępowe, serwery terminali, serwery VPN, system backupowy, system NAC,
- c) monitorowanie zdarzeń naruszenia cyberbezpieczeństwa w trybie 24 / 7 / 365 przez system SIEM ,
- d) przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji,
- e) analiza i eliminacja najprostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji,
- f) łączenie (korelowanie) zdarzeń oraz incydentów cyberbezpieczeństwa,
- g) reagowanie na wykryte incydenty, analiza incydu, klasyfikacja incydu, obsługa incydu,
- h) zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive),
- i) nadawanie priorytetu i kategoryzowanie zdarzeń bezpieczeństwa,
- j) przygotowywanie miesięcznych raportów wykrytych zdarzeń bezpieczeństwa,
- k) analizę zdarzeń zagrażających bezpieczeństwu danych lub systemów,
- l) przygotowywanie i realizację Scenariuszy użycia systemu bezpieczeństwa,
- m) przygotowanie Scenariuszy Reakcji,



## OKRĘGOWY SZPITAL KOLEJOWY W KATOWICACH

Samodzielny Publiczny Zakład Opieki Zdrowotnej

40-760 Katowice, ul. Panewnicka 65

tel.: 32 605 35 00, fax: 32 605 35 08

NIP 634-23-05-444 REGON 276267686 NR BDO: 000054612



Jednostka Ochrony Zdrowia  
Samorządu Województwa Śląskiego

- n) przygotowanie raportów incydentalnych oraz raportów na żądanie Zamawiającego.
- o) przygotowanie zaleceń po wykonaniu analizy środowiska, testów podatności oraz testów penetracyjnych. Testy penetracyjne obejmują testy zewnętrzne, wewnętrzne oraz aplikacyjne;
- p) analiza przyczynowa (Root Cause Analysis) zdarzeń zagrażających bezpieczeństwu danych,
- q) raportowanie incydentów bezpieczeństwa do osób i organów zewnętrznych, wskazanych każdorazowo przez Zamawiającego,
- r) ocena skuteczności zaimplementowanych środków bezpieczeństwa,
- s) Tworzenie polityk i procedur analizy ryzyka oraz bezpieczeństwa IT.
- t) Proponowanie rozwiązań mających na celu uzyskać zgodność z przepisami i standardami (NIS2, KSC i powiązanych aktów prawnych, RODO, ISO/IEC).
- u) Monitorowanie ciągłości działania systemów krytycznych (sprzęt, oprogramowanie, bazy danych), poprzez wdrożenie narzędzi do monitoringu infrastruktury IT,

