Wstępny OPZ audyt i bezpieczeństwo

Cz. I – Radom, Ciechanów, Bródno; cz. II – Konstancin, Pruszków; cz. III – Siedlce, Rudka.

Czas na realizację zamówienia (dla każdej części): do 7 miesięcy od dnia podpisania umowy.

DZIAŁANIA ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM Systemu aptecznego[1]

I. Audyty bezpieczeństwa i budowa dokumentacji zgodnej z wymaganiami normy ISO/IEC 27001:2013 lub równoważną oraz ciągłością działania usługi kluczowej wytworzoną zgodnie z wymaganiami normy PN-EN ISO 22301 lub równoważnej.

1. Przeprowadzanie w ciągu dwóch miesięcy od podpisania umowy audytu wstępnego bezpieczeństwa i ciągłości działania w podmiocie w obszarze oddziaływania projektu. Audyt przeprowadza zespół:
    a) Koordynator Testów Bezpieczeństwa, który:
        - Posiada co najmniej 3 letnie doświadczenie w przeprowadzaniu testów bezpieczeństwa aplikacji i infrastruktury,
        - Posiada certyfikat Certified Ethical Hacker (CEH) lub równoważny,
        - Posiada certyfikat Offensive Security Certified Professional (OSCP) lub równoważny,
        - Przeprowadził co najmniej 5 testów bezpieczeństwa systemów informatycznych e-usług wraz z infrastrukturą w podmiotach leczniczych.
    b) osoba pełniąca funkcję audytora spełniająca łącznie wszystkie poniższe warunki:
        - Posiada certyfikat audytora wiodącego ISO/IEC 22301 lub równoważny,
        - Posiada certyfikat audytora wiodącego ISO/IEC 27001 lub równoważny,
        - Posiada co najmniej 5 – letnie doświadczenie zawodowe w zakresie audytowania zgodnie z wymaganiami normy PN-ISO/IEC 27001 oraz ISO/IEC 22301 lub równoważnymi,
        - Uczestniczyła w co najmniej dwóch wdrożeniach lub audycie zgodnie z wymaganiami normy PN-ISO/IEC 27001 lub ISO/IEC 22301 lub równoważnych dla jednostek z branży ochrony zdrowia,
        - Uczestniczyła w co najmniej trzech audytach przeprowadzonych zgodnie z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560 z późn. zm. – dalej „KSC") dla jednostek z branży ochrony zdrowia.
    c) osoba pełniąca funkcję audytora spełniająca łącznie wszystkie poniższe warunki:
        - Posiada certyfikat audytora wiodącego ISO/IEC 27001 lub równoważny,
        - Posiada co najmniej 3 – letnie doświadczenie zawodowe w zakresie audytowania zgodnie z wymaganiami normy PN-ISO/IEC 27001 lub równoważnej,
        - Uczestniczyła w co najmniej jednym wdrożeniu lub audycie Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami normy

[1] System apteczny w rozumieniu definicji przedstawionych w umowach na konkretne części zamówienia publikowane po d adresami: https://mss.ezamawiajacy.pl/pn/mss/demand/notice/public/31735/details, https://mss.ezamawiajacy.pl/pn/mss/demand/notice/public/25740/details i https://mss.ezamawiajacy.pl/pn/mss/demand/notice/public/21010/details.

PN-ISO/IEC 27001 lub równoważnej dla jednostek z branży ochrony zdrowia,
- Uczestniczyła w co najmniej trzech audytach przeprowadzonych zgodnie z KSC dla jednostek z branży ochrony zdrowia,
- posiada certyfikat ukończenia szkolenia z zakresu ISO 27701:2019 lub równoważnego,
- posiada certyfikat ukończenia szkolenia z zakresu ISO/IEC 27017 lub równoważnego z elementami ochrony danych osobowych przetwarzanych w chmurze (ISO/IEC 27018 lub równoważnej).

Audyt kończy się sporządzeniem raportu zawierającego ustalenia co do stanu zastanego i rekomendacje co do stanu oczekiwanego, w szczególności w kontekście wymogów KSC i aktów wykonawczych[2] oraz rekomendacji CSIOZ/CEZ i niezbędnej dokumentacji oraz optymalnej konfiguracji oprogramowania planowanego do wdrożenia w ramach projektu.

2. Budowa dokumentacji zgodnej z wymaganiami normy ISO/IEC 27001:2013 lub równoważnej oraz ciągłością działania usługi kluczowej wytworzoną zgodnie z wymaganiami normy PN-EN ISO 22301 lub równoważnej, w szczególności:
   a) Dokumentacji systemu zarządzania bezpieczeństwem informacji (ISO 27001),
   b) Dokumentacji ochrony infrastruktury wykorzystywanej do świadczenia usługi,
   c) Dokumentacji zarządzania ciągłością działania usługi (ISO 22301), w tym opracowanie strategii zapewnienia ciągłości działania dla usług reagowania na incydenty (art. 14 KSC) oraz usługi zarządzania lekami, produktami leczniczymi i wyrobami medycznymi oraz opracowanie planów ciągłości działania dla zarządzania lekami, produktami leczniczymi i wyrobami medycznymi,
   d) Opis sposobów dokumentowania czynności w ramach ustalonych procedur,
   e) Procedury nadzoru nad dokumentacja dotyczącą cyberbezpieczeństwa.
3. procedury zarządzania bezpieczeństwem informacji w ramach obrotu lekami, produktami leczniczymi i wyrobami medycznymi (art. 14 KSC). Przeprowadzenie szacowania ryzyka wystąpienia incydentu cyberbezpieczeństwa usług zarządzania lekami, produktami leczniczymi i wyrobami medycznymi (art. 8 KSC).
4. Opracowanie systemu zarządzania (w tym klasyfikacji i obsługi) incydentami zgodnie z art. 8 i 11 KSC.
5. Przeprowadzenie analizy wpływu na biznes (BIA) dla usług zarządzania lekami, produktami leczniczymi i wyrobami medycznymi.
6. Opracowanie procedur wspierających politykę bezpieczeństwa informacji w obszarze Systemu aptecznego uwzględniających co najmniej:
   a) Określenie osób do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa i przekazanie ich danych do organu ds. cyberbezpieczeństwa zgodnie z art. 9 KSC,
   b) Powołanie wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo o kompetencjach wymaganych w KSC w szczególności zgodnie z art. 14 KSC,

[2] rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. 2018 poz. 2180), rozporządzanie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. 2018 poz. 2080), rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.

c) Przygotowanie propozycji składu, określenie ról i zadań zespołu wykonawczego po stronie Zamawiającego,
d) Określenie sposobu dostosowania pomieszczeń,
e) Określenie odpowiednich i adekwatnych do oszacowanego ryzyka środków technicznych i organizacyjnych w obszarze utrzymania i eksploatacji systemu, bezpieczeństwa fizycznego i środowiskowego oraz bezpieczeństwa i ciągłość dostaw usług, od których zależy świadczenie usługi,
f) Wskazanie optymalnego sposobu zapewnienia personelowi dostępu do wiedzy w zakresie cyberbezpieczeństwa zgodnie z art. 9 KSC,
g) Procedurę zgłaszania incydentu poważnego niezwłocznie, nie później niż w ciągu 24 h od momentu jego wykrycia do Zespołu reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), (art. 11 KSC),
h) Procedurę zapewniania wsparcia wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo w trybie całodobowym przez wszystkie dni w roku (art. 14 KSC),
i) Zapewnienie dostępu do informacji o rejestrowanych incydentach dla CSIRT (art. 11 KSC),
j) Procedurę współdziałania z CSIRT podczas obsługi incydentu poważnego i krytycznego (art. 11 KSC).
k) Zapewnienie przechowywania dokumentacji dotyczącej cyberbezpieczeństwa przez co najmniej 2 lata od dnia jej wytworzenia,
l) Określenie polityki logowania i retencji zapisów zdarzeń w systemach informatycznych w usługach zarządzania lekami, produktami leczniczymi i wyrobami medycznymi.

7. Opracowanie procedur i wzorów dokumentów zapewniających zgodność przetwarzania danych osobowych w chmurze szyfrowanej, o której mowa niżej z RODO (w tym ustalenie podstaw i zakresu przetwarzania, retencji danych, wzorów klauzul informacyjnych i pozostałych wymogów RODO).
8. Zapewnienie ciągłego monitorowania systemów informatycznych dostarczonych w ramach projektu realizowane przez zespół zarejestrowany w Trusted Introducer w okresie Wsparcia (równego okresowi gwarancji, min. 24 miesiące).
9. Zapewnienie automatycznego generowania dziennych raportów z monitorowania podatności systemów IT wykorzystywanych dla usług zarządzania lekami, produktami leczniczymi i wyrobami medycznymi na incydenty systemu informatycznego.
10. Zapewnienie wsparcia przy obsłudze incydentów bezpieczeństwa w systemie aptecznym, w tym zapewnienie oprogramowania lub usługi analizy kodu szkodliwego oprogramowania i zabezpieczania śladów kryminalistycznych – w okresie Wsparcia (równego okresowi gwarancji, min. 24 miesiące)..

12. Przeprowadzenie zapewniającego audytu bezpieczeństwa zamykającego projekt. Audyt przeprowadza zespół analogiczny do określonego w pkt. 1 a)-c). Audyt kończy się sporządzeniem raportu zawierającego ustalenia co do stanu zastanego, weryfikujące właściwe wdrożenie działań związanych z cyberbezpieczeństwem rekomendowanych w wyniku przeprowadzania audytu, o którym mowa w pkt 1, w tym istnienie właściwych procedur oraz prawidłowe funkcjonowanie nw. oprogramowania i chmury szyfrowanej.

II. Dostawa chmury szyfrowanej do przechowywania kopii zapasowych zgodna z rekomendacjami CSIOZ/CEZ

Poniższa specyfikacja w rozbiciu na części:
Część I: 3x (1x Radom, 1x Ciechanów, 1 X Warszawa – Bródno) – 3x 100 TB szyfrowanej przestrzeni dyskowej.
Część II: 1x (obejmuje lokalizacje Konstancin i Pruszków) – 1x 100 TB szyfrowanej przestrzeni dyskowej.
Część III: 1x (obejmuje lokalizacje Siedlce i Rudka) – 1 x 100 TB szyfrowanej przestrzeni dyskowej.

Dostawa polega na udostępnieniu dla klienta przestrzeni dyskowej, na której dane przechowywane są w postaci zaszyfrowanej. Usługa powinna zapewnić dostęp dla lokalizacji Partnerów Projektu zgodnie z ww. Każdy z Partnerów Projektu powinien posiadać niezależny dostęp jak i możliwość przydzielania powierzchni użytkownikom.
Licencja powinna pozwalać na korzystanie z chmury kryptograficznej przez okres co najmniej zaoferowanego okresu gwarancji (min. 24 miesiące).

Wymagania minimalne:

Infrastruktura dostawcy	Wielopoziomowe bezpieczeństwo: - spełnia normę EN 50600 co najmniej w 3 klasie w zakresie wyposażenia i infrastruktury – systemy zabezpieczeń lub normę równoważną - szyfrowanie połączenia pomiędzy klientem a infrastrukturą dostawcy usługi (długość klucza min. 2048bit), - szyfrowanie danych znajdujących się na przestrzeni udostępnionej klientowi, - szyfrowanie całej infrastruktury dedykowanej klientowi; Min. jedna dedykowana do przechowywania danych serwerownia (centrum przetwarzania danych) na terenie Unii Europejskiej. Niedopuszczalne jest, aby dostawca usługi świadczył oferowane usługi chmury szyfrowanej w oparciu o infrastrukturę rozproszoną firm trzecich. Centrum Przetwarzania Danych dostawcy usługi powinno posiadać minimum poniższe parametry: - aktywne elementy infrastruktury IT zapewniające pracę w modelu n+1; - redundantne wewnętrzne linie dystrybucji energii elektrycznej obsługujące urządzenia w szafie RACK; - redundantne wewnętrzne linie chłodu równolegle obsługujące urządzenia w szafie RACK; - każdy element linii dystrybucji energii elektrycznej i chłodu może być odłączony w celu poddania czynnościom serwisowym bez wpływu na normalną pracę urządzeń dwuzasilaczowych; - w Centrum Przetwarzania Danych musi być wdrożona strefowa kontrola dostępu w oparciu o karty zbliżeniowe lub rozwiązanie równoważne; - wymagana jest całodobowa ochrona fizyczna Centrum Przetwarzania Danych z rejestracją kamer na zewnątrz i wewnątrz budynku; - dzierżawione środowisko musi być umiejscowione w Centrum Przetwarzania Danych zlokalizowanego na terenie Unii Europejskiej; - Centrum Przetwarzania Danych musi posiadać niezależne strefy pożarowe oraz system wczesnej detekcji dymu i ognia, a pomieszczenie kolokacji musi być wyposażone w zautomatyzowaną aparaturę gaśniczą;

	- Centrum Przetwarzania Danych musi mieć zapewnione zasilanie z dwóch niezależnych linii energetycznych oraz rezerwowe zasilanie realizowane przy pomocy UPS oraz minimum jednego agregatu prądotwórczego; - wymagane jest, aby dystrybucja energii elektrycznej do każdej z szaf RACK odbywała się z wykorzystaniem minimum dwóch niezależnych torów zasilania, z minimum jednym torem gwarantowanym (podtrzymanie zasilania z wykorzystaniem UPS i agregatu prądotwórczego). W ramach zapewnienia podwyższonego bezpieczeństwa dla krytycznych danych (dane medyczne, dane osobowe, dane finansowe) dostawca powinien zapewnić możliwość tworzenia kopii przechowywanych danych – system powinien pozwalać na wybór danych istotnych dla klienta. Dostawca usługi powinien zapewnić możliwość udostępnienia dodatkowej infrastruktury pozwalającej na odtworzenie kopi zapasowej danych klienta (bez ingerencji w produkcyjne dane przechowywane w chmurze kryptograficznej). Dostawca usługi powinien zagwarantować, że serwer nie jest w stanie uzyskać dostępu do plików klienta w postaci jawnej (serwer nie posiada, ani nie może wyznaczyć żadnego z kluczy kryptograficznych klienta usługi). Dostawca usługi powinien gwarantować, że klient nie jest w stanie wykonać żadnej operacji kryptograficznej na swoim kluczu prywatnym (podpisu, deszyfrowania) bez udziału serwera.
Parametry ogólne	Typ usługi: przestrzeń dyskowa w chmurze z szyfrowaniem na trzech poziomach (połączenie, dane, infrastruktura) Powierzchnia: 100TB na Partnera Projektu – zgodnie z ww. specyfikacją z możliwością zwiększania co 1 TB (za dodatkową opłatą per TB) z czasowym użyczeniem licencji na okres równy okresowi gwarancji (min. 24 miesięcy) dla oprogramowania służącego do bezpiecznego przesyłania i współdzielenia plików w ramach struktury organizacyjnej Zamawiającego dla nieograniczonej liczby urządzeń. Rozwiązanie technologiczne musi być zgodne z: - Rekomendacjami Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej, - Kodeksem postępowania dla sektora ochrony zdrowia wydanym zgodnie z art. 40 RODO dotyczącym podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających. Rozwiązanie powinno być rozwiązaniem bezpiecznym opartym o technologię kryptograficznej ochrony danych, gwarantującej podwyższony poziom ochrony kluczy szyfrujących, który realizowany będzie poprzez technologię zapewniającą, że nie będą one nigdy przetrzymywane w całości w jednym miejscu.

Obsługiwane protokoły	Dostęp do usługi chmury kryptograficznej powinien być zapewniony co najmniej za pomocą protokołów: iSCSI SFTP HTTPS (HTTP over SSL) WebDAV SSL IPSec SMB
Zarządzanie użytkownikami	Tworzenie użytkowników Usuwanie użytkowników Tworzenie grup Usuwanie grup Wyłączenia/Włączanie kont użytkowników
Panel Sterowania	Dostępny przez WWW Obsługa protokołu HTTPS Możliwość dostępu do panelu: - z dedykowanego adres IP - z dedykowanego urządzenia - tylko po zestawieniu tunelu szyfrowanego Edycja danych przedsiębiorstwa/klienta Zarządzanie dostępną przestrzenią dyskową (możliwość zwiększenia/zmniejszenia) Zarządzanie wykupionymi usługami Zarządzania funkcją backupu infrastruktury Zarządzanie udostępnionymi folderami Możliwość podglądu fizycznej lokalizacji danych Możliwość zmiany fizycznej lokalizacji danych (między serwerowniami dostawcy usługi) Zarządzanie kanałami dostępu (iSCSI, SFTP, HTTPS, WebDAV, SMB)
Bezpieczeństwo	Obsługa zdalnego peera: zgodni z IPsec klienci dial-up, peery ze statycznym adresem IP / dynamicznym DNS Metoda uwierzytelniania: certyfikat, klucz współdzielony IPsec Phase 1: tryb agresywny i główny (ochrona identyfikatora) Obsługa IKEv1, IKEv2 (RFC 4306) Konfigurowalny port IKE Szyfrowanie propozycji fazy 1 / fazy 2: DES, 3DES, AES128. AES192, AES256, ARIA128, ARIA192, ARIA256, SEED Uwierzytelnianie propozycji fazy 1 / fazy 2: MD5, SHA1, SHA256, SHA384, SHA512 Obsługa Faza 1 / Faza 2 Diffie-Hellman Group: 1, 2, 5, 14 do 21, 27 do 32 Obsługa ChaCha20 / Poly1305 PRF: SHA1, SHA256, SHA384 i SHA512 Konfigurowalne wygaśnięcie klucza szyfrowania IKE, częstotliwość utrzymywania aktywności translacji NAT Fragmentacja IP przed / po hermetyzacji IPsec Wykrywanie Dead Peer Wsparcie dla certyfikatów RSA SelfSigned: klucze 1k/2k/4k/8k/16k bitowe Wsparcie dla certyfikatów ECC: klucze 256/384/521bitowe Obsługa certyfikatów X.509 Obsługa wewnętrznego CA Szyfrowanie infrastruktury za pomocą algorytmu AES256

	Możliwość wykorzystania czytników kart Każdy użytkownik otrzymuje indywidualny certyfikat do szyfrowania i deszyfrowania danych
Dostęp do plików	Tylko dla użytkowników posiadających aktywne konto w systemie Tylko dla użytkowników posiadających ważny certyfikat wygenerowany przez system (administratora) Tylko dla użytkowników z odpowiednimi prawami dostępu (RO/RW) Dostęp do plików: - z poziomu powłoki Windows - w poziomu przeglądarki WWW
Inspekcja czynności	Zapewnienie logów systemowych - zestawienia tunelu - dostęp do zasobów - logowanie do panelu Logi powinny pozwalać na jednoznaczną identyfikację użytkownika, zasobu, datę i godzinę.
Instalator i aplikacja kliencka	Dostawca usługi powinien zapewnić dedykowany dla klienta instalator, który poprowadzi przez proces instalacji potrzebnego oprogramowania na stacji klienckiej. Niedopuszczalne jest stosowanie dedykowanej aplikacji klienckiej. Usługa powinna być zintegrowana z powłoką systemu Windows a instalator powinien wykonać wszystkie czynności niezbędne do integracji z usługą chmury szyfrowanej (w tym zainstalować odpowiedni certyfikat użytkownika na stacji klienckiej) Instalator powinien umieścić odpowiedni skrót na pulpicie komputera pozwalający na dostęp do szyfrowanego foldera w chmurze kryptograficznej
Integracja z MS ActiveDirecotry	Możliwość wykorzystania istniejących w infrastrukturze klienta kont w ActiveDirectory do celów autoryzacji do usług chmurowych. Szyfrowany kanał komunikacyjny między Infrastrukturą klienta a infrastruktur dostawcy usługi: - zestawiany za pomocą dedykowanego instalatora - zestawiany za pomocą urządzenia typu koncentrator VPN (Firewall) przy wykorzystaniu protokołu IPSEC
Integracja ze sprzętem i oprogramowaniem firm trzecich	Dostawca usługi powinien zapewnić możliwość integracji z urządzeniami i oprogramowaniem firm trzecich, w tym: - współpracę z oprogramowaniem do tworzenie kopii zapasowych Veeam oraz Nakivo - współpracę ze sprzętem sieciowym firm minimum HPE, Aruba, Fortinet - możliwość automatyzacji wykonywania kopii konfiguracji przy pomocy gotowych (dostarczanych przez dostawcę usługi) skryptów dla posiadanych minimum urządzeń: - Aruba 25xx, 2930x, 38xx, 54xx - Aruba CX 61xx, 62xx, 63xx, 83xx - Fortinet Fortigate
Gwarancja i wsparcie	Min. 24 miesiące gwarancji oraz wsparcia dostawcy usługi Wykonawca zobowiązany jest w trakcie trwania umowy licencyjnej (wsparcie dostawcy usługi – równe zaoferowanemu terminowi gwarancji, min. 24 miesiące): 1) Dostarczać Zamawiającemu nowsze wersje oprogramowania, uaktualnienia oraz „support packi” poprzez wskazanie miejsca do

	pobrania i przesłania informacji drogą mailową, wraz z instrukcją instalacji i listą zmian – release notes; 2) Świadczyć usługi opieki serwisowej oraz wsparcia oprogramowania także na nowszych wersjach oprogramowania – dostarczonych w ramach umowy; 3) Udzielić wsparcia w trakcie instalacji dokonywanych przez Zamawiającego dostarczonego oprogramowania oraz poprawek; 4) Zapewnić rozwiązywanie problemów związanych z instalacją i funkcjonowaniem dostarczonego oprogramowania; 5) Zapewnić przyjmowanie zgłoszeń telefonicznych potwierdzanych zgłoszeniem elektronicznym (www lub e-mail) w trybie 24x7x365 od Zamawiającego z zachowaniem minimalnych warunków przyjęcia zgłoszenia, przez Wykonawcę, tj.: o w godzinach pomiędzy 08:00 a 16.00 dnia roboczego – zgłoszenie traktowane jest jak przyjęte danego dnia roboczego; o w godzinach pomiędzy 16.00 a 24.00 dnia roboczego – zgłoszenie traktowane jest jak przyjęte o godz. 8.00 następnego dnia roboczego; o w godzinach pomiędzy 0.00 a 8.00 dnia roboczego - zgłoszenie traktowane jest jak przyjęte o godz. 8.00 danego dnia roboczego; o w dniu ustawowo lub dodatkowo wolnym od pracy - zgłoszenie traktowane jest jak przyjęte o godz. 8.00 najbliższego dnia roboczego; o Nie później niż w ciągu 30 minut od momentu otrzymania zgłoszenia awarii potwierdzić przyjęcie zgłoszenia; 6) Zapewnić czas reakcji na zgłoszone problemy, rozumiany jako przesłanie szczegółowego planu działania naprawczego Wykonawcy w związku z dokonanym zgłoszeniem przy zgłoszeniu: o błędu krytycznego do 12 godzin od momentu zgłoszenia, o błędu niekrytycznego naprawa powinna nastąpić w najbliższym wydaniu oprogramowania. o status zgłoszenia określa Zamawiający, wg poniższych kryteriów: o błąd krytyczny – nie można zaszyfrować/odszyfrować danych; o błąd niekrytyczny – pozostałe błędy; 7) Zapewnić dostęp do bazy wiedzy o dostarczonym oprogramowaniu; 8) Zapewnić e-mail'owe i telefoniczne konsultacje w zakresie dostarczonego oprogramowania we wszystkie dni robocze w godz. 9.00 – 17.00

III. OPROGRAMOWANIE z obszaru cyberbezpieczeństwa

1. Oprogramowanie wspierające automatyczne rejestrowanie zgłoszeń incydentów bezpieczeństwa oraz obsługę zdarzeń o funkcjonalnościach wskazanych poniżej
2. Oprogramowanie do monitorowania podatności w systemach teleinformatycznych.
3. Oprogramowanie do automatycznego wykrywania przypadków naruszenia bezpieczeństwa eUsług o funkcjonalnościach:
4. Oprogramowanie do badania odporności systemów informacyjnych na przełamywanie zabezpieczeń

5. Oprogramowanie do nadzorowania i realizacji audytów bezpieczeństwa i działań podejmowanych w ich wyniku o funkcjonalnościach
6. Oprogramowanie do monitorowania systemów teleinformatycznych wykorzystywanych do świadczenia eUsług z funkcją korelacji zdarzeń bezpieczeństwa o funkcjonalnościach.

LICENCJE OPROGRAMOWANIE

Dla każdego z 6 ww. oprogramowań: 1 licencja dla każdego Partnera Projektu dla nieograniczonej liczby urządzeń/ użytkowników:

Część I – łącznie 3 x 6 licencji :
Radom –licencje x1
Ciechanów – licencje x1
Warszawa Bródno – licencje x1

Część II – łącznie 1x6 licencji:
Konstancin, Pruszków – licencje x1

Część III – łącznie 1x6 licencji:
Siedlce, Rudka – licencje x1

FUNKCJONALOŚCI SYSTEMÓW

1. <u>Oprogramowanie wspierające automatyczne rejestrowanie zgłoszeń incydentów bezpieczeństwa oraz obsługę zdarzeń o funkcjonalnościach:</u>

1) Oprogramowanie musi dostarczone w formule SaaS na czas świadczenia usługi w ramach umowy.
2) Oprogramowanie jest zgodne z adekwatnymi przepisami prawa[3] oraz w okresie wsparcia dostawcy gwarantuje stałą, pełną zgodność wszelkich realizowanych funkcji/algorytmów rozliczeń/formatów sprawozdań z obowiązującym prawem, dostosowywanie oprogramowania do zmian przepisów obowiązującego odbywa się z odpowiednim wyprzedzeniem.
3) Oprogramowanie jest dostarczone przez oferenta i nie narusza praw licencyjnych innych osób i podmiotów
4) Oprogramowanie umożliwia pracę terminalową poprzez przeglądarkę.
5) Oprogramowanie komunikuje się z użytkownikiem w języku polskim i angielskim.
6) Dokumentacja użytkowa jest zgodna ze stanem faktycznym.
7) Oprogramowanie posiada funkcjonalności zapewniające bezpieczeństwo informacji:
   a) posiada wbudowany mechanizm autoryzacji, posiada mechanizmy zabezpieczające przed nieautoryzowanym dostępem.
   b) Posiada funkcjonalność zarządzania i administrowania uprawnieniami, w szczególności: mechanizm nadawania uprawnień funkcjonalnych do poszczególnych obszarów każdemu użytkownikowi,

[3] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 r. poz. 1560 z późn. zm., rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. 2018 poz. 2180), rozporządzanie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. 2018 poz. 2080), rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych oraz rekomendacji CSIOZ/CEZ.

8) Możliwość automatycznego rejestrowania zdarzeń z wykorzystaniem narzędzi zewnętrznych oraz możliwość ręcznego wprowadzenia zdarzenia do oprogramowania
9) Oprogramowanie zapewnia udostępnienie danych innym systemom i dedykowanym odbiorcom z wykorzystaniem komunikacji email oraz interfejsu do wymiany danych (web service).
10) Oprogramowanie umożliwia śledzenie zdarzeń i czasów ich obsługi, otrzymywanie alertów i powiadomień o niedotrzymanych terminach.
11) Oprogramowanie umożliwia administratorowi łatwe utrzymanie zbioru standardowych raportów.
12) Raporty przeglądu oprogramowania i podstawowych statystyk dotyczących liczby zgłoszeń i statusu w podziale na jednostki organizacyjne, kolejki, tematy.
13) Możliwość wyświetlania szczegółowych informacji o danych zdarzeniach.
14) Obsługa oprogramowania w czasie zbliżonym do rzeczywistego.
15) Każdemu użytkownikowi można zdefiniować odrębny zakres dostępu.

2. Oprogramowanie do monitorowania podatności w systemach teleinformatycznych

1) Narzędzie musi dostarczone w formule SaaS na czas świadczenia usługi w ramach umowy.
2) Oprogramowanie jest zgodne z adekwatnymi przepisami prawa[4] oraz w okresie wsparcia dostawcy gwarantuje stałą, pełną zgodność wszelkich realizowanych funkcji/algorytmów rozliczeń/formatów sprawozdań z obowiązującym prawem, dostosowywanie oprogramowania do zmian przepisów obowiązującego.
3) Narzędzie jest własnością Wykonawcy i nie narusza praw licencyjnych innych osób i podmiotów.
4) Umożliwia pracę terminalową poprzez przeglądarkę. Narzędzie komunikuje się z użytkownikiem w języku polskim i angielskim.
5) Dokumentacja użytkowa jest zgodna ze stanem faktycznym.
6) Narzędzie posiada funkcjonalności zapewniające bezpieczeństwo informacji: posiada wbudowany mechanizm autoryzacji, posiada mechanizmy zabezpieczające przed nieautoryzowanym dostępem.
7) Narzędzie posiada funkcjonalności umożliwiające planowe wykonywanie kopii zapasowych danych bez konieczności wylogowania użytkowników.
8) Posiada funkcjonalność zarządzania i administrowania uprawnieniami, w szczególności: mechanizm nadawania uprawnień funkcjonalnych do poszczególnych obszarów każdemu użytkownikowi, możliwość nadawanie użytkownikom.
9) Narzędzie zapewnia udostępnienie danych innym systemom w formie i zakresie ustalonym przez użytkownika wykorzystując jeden ze standardowych formatów wymiany danych, co najmniej xls.

[4] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 r. poz. 1560 z późn. zm., rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. 2018 poz. 2180), rozporządzanie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. 2018 poz. 2080), rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych oraz rekomendacji CSIOZ/CEZ.

10) Narzędzie zapewnia drukowanie raportów w formie i zakresie ustalonym przez użytkownika wykorzystując jeden ze standardowych formatów wymiany danych, co najmniej PDF, xls.
11) Narzędzie umożliwia administratorowi łatwe utrzymanie zbioru standardowych raportów (dodawanie, modyfikowanie, usuwanie raportów).
12) W miejscach Interfejsu użytkownika, w których prezentowane są dane w formie tabelarycznej jest możliwość sortowania danych i zmiany kryteriów wyszukiwania.
13) Możliwość wyświetlania szczegółowych informacji, o podatnościach systemów IT.
14) Obsługa wyszukiwania w czasie zbliżonym do rzeczywistego.
15) Każdemu użytkownikowi można zdefiniować odrębny zakres raportów.

3. Oprogramowanie do automatycznego wykrywania przypadków naruszenia bezpieczeństwa eUsług o funkcjonalnościach:

1) Oprogramowanie musi dostarczone w formule SaaS na czas świadczenia usługi w ramach umowy (min. 24 m-ce - świadczenia równy zaoferowanemu okresowi gwarancji).
2) Oprogramowanie jest zgodne z adekwatnymi przepisami prawa[5] oraz w okresie wsparcia dostawcy gwarantuje stałą, pełną zgodność wszelkich realizowanych funkcji/algorytmów rozliczeń/formatów sprawozdań z obowiązującym prawem,
3) Oprogramowanie jest własnością oferenta i nie narusza praw licencyjnych innych osób i podmiotów.
4) Oprogramowanie umożliwia pracę terminalową poprzez przeglądarkę.
5) Dokumentacja użytkowa jest zgodna ze stanem faktycznym.
6) Oprogramowanie posiada funkcjonalności zapewniające bezpieczeństwo informacji:
   a) posiada wbudowany mechanizm autoryzacji, posiada mechanizmy zabezpieczające przed nieautoryzowanym dostępem.
   b) Użytkownik przy użyciu interfejsu dodaje adresy witryn internetowych eUsług, które są następnie monitorowane.
7) Oprogramowanie posiada funkcjonalność obliczania ryzyka wystąpienia ataku na eUsługę na podstawie co najmniej 6 parametrów.
8) Oprogramowanie w celu obliczenia ryzyka wystąpienia ataku pobiera i zapisuje na serwerze zawartość monitorowanej witryny internetowej eUsługi, wraz z plikami graficznymi oraz zrzuty ekranu (screenshoty) monitorowanej witryny internetowej eUsługi.
9) Oprogramowanie monitoruje witryny internetowej eUsługi, przeprowadzając obserwacje w regularnych odstępach czasu, nie dłuższych niż 60 minut.
10) Użytkownik ma możliwość tymczasowego wyłączenia monitorowania witryny internetowej eUsługi.
11) Oprogramowanie umożliwia przegląd wyników monitorowania w formie tabeli oraz wykresów.

[5] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 r. poz. 1560 z późn. zm., rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. 2018 poz. 2180), rozporządzanie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. 2018 poz. 2080), rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych oraz rekomendacji CSIOZ/CEZ.

12) Oprogramowanie pozwala na zdefiniowanie dla każdej monitorowanej witryny internetowej eUsługi progu dla wyliczonej wartości ryzyka, którego osiągnięcie lub przekroczenie skutkuje wygenerowaniem powiadamiania (w przypadku braku wskazania, próg przyjmuje wartość domyślną).
13) W przypadku braku wskazania progu dla wyliczonej wartości ryzyka, przyjmuje on wartość domyślną.
14) Oprogramowanie wysyła powiadomienie ostrzegawcze (alert) na adres e-mail użytkownika, gdy wyliczona wartość ryzyka osiągnie lub przekroczy wskazany próg powiadamiania.
15) Oprogramowanie wysyła powiadomienie ostrzegawcze (alert) o niedostępności witryny internetowej eUsługi na adres e-mail użytkownika, gdy oprogramowanie nie będzie w stanie pobrać jej zawartości przez 3 kolejne cykle monitorowania.
16) Oprogramowanie zapewnia możliwość wygenerowania raportu w formacie PDF na życzenie użytkownika, obejmującego wybrany przedział czasowy.
17) Oprogramowanie zapewnia możliwość okresowego wysyłania raportu w formacie PDF na adres e-mail użytkownika.
18) Obsługa oprogramowania w czasie zbliżonym do rzeczywistego.

4. Oprogramowanie do badania odporności systemów informacyjnych na przełamywanie zabezpieczeń o funkcjonalnościach:

1) Oprogramowanie musi dostarczone w formule SaaS na czas świadczenia usługi w ramach umowy.
2) Oprogramowanie jest zgodne z adekwatnymi przepisami prawa[6] oraz w okresie wsparcia dostawcy gwarantuje stałą, pełną zgodność wszelkich realizowanych funkcji/algorytmów rozliczeń/formatów sprawozdań z obowiązującym,
3) Oprogramowanie jest stworzone przez oferenta lub ma prawo do udzielenia licencji i nie narusza praw licencyjnych innych osób i podmiotów.
4) Oprogramowanie umożliwia pracę terminalową poprzez przeglądarkę.
5) Dokumentacja użytkowa jest zgodna ze stanem faktycznym.
6) Oprogramowanie posiada funkcjonalności zapewniające bezpieczeństwo informacji: posiada wbudowany mechanizm autoryzacji, posiada mechanizmy zabezpieczające przed nieautoryzowanym dostępem,
7) Oprogramowanie pozwala wykrywanie usług w sieci z wykorzystaniem różnych protokołów komunikacji.
8) Oprogramowanie znajduje otwarte porty w sieci użytkownika.
9) Oprogramowanie skanuje system użytkownika pod kątem wykrywania podatności o różnych stopniach zagrożenia.
10) Oprogramowanie podaje opis oraz prawdopodobne skutki występowania podatności, jak również rozwiązania potrzebne do ich wyeliminowania.

[6] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 r. poz. 1560 z późn. zm., rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. 2018 poz. 2180), rozporządzanie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. 2018 poz. 2080), rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych oraz rekomendacji CSIOZ/CEZ.

11) Oprogramowanie tworzy raporty w formacie PDF zawierające podsumowanie skanowania w języku angielskim.
12) Oprogramowanie komunikuje się z użytkownikiem tylko w języku polskim i angielskim.
13) Użytkownik może skanować system wszystkimi narzędziami na raz, jak również wybrać poszczególne funkcje z listy.
14) Oprogramowanie pozwala na automatyczne wykonywanie okresowego skanowania w odstępach czasu określonych przez użytkownika.
15) Oprogramowanie sprawdza siłę danych dostępu w systemach użytkownika, korzystając z list popularnych loginów i haseł.
16) Wyniki działania narzędzi zawartych w oprogramowaniu wyświetlają się na ekranie głównym użytkownika.
17) Oprogramowanie pozwala na wysłanie wyników skanowania drogą mailową.
18) Oprogramowanie pozwala na dostęp do raportów z wcześniejszych skanowań przez 12 miesięcy.
19) Oprogramowanie zapewnia możliwość wygenerowania raportu w formacie PDF.
20) Oprogramowanie zapewnia możliwość okresowego wysyłania raportu w formacie PDF na adres e-mail użytkownika.
21) Obsługa oprogramowania w czasie zbliżonym do rzeczywistego.

5. Oprogramowanie do nadzorowania i realizacji audytów bezpieczeństwa i działań podejmowanych w ich wyniku o funkcjonalnościach:

1) Oprogramowanie musi dostarczone w formule SaaS na czas świadczenia usługi w ramach umowy.
2) Oprogramowanie jest zgodne z adekwatnymi przepisami prawa[7] oraz w okresie wsparcia dostawcy gwarantuje stałą, pełną zgodność wszelkich realizowanych funkcji/algorytmów rozliczeń/formatów sprawozdań z obowiązującym prawem.
3) Oprogramowanie jest własnością oferenta i nie narusza praw licencyjnych innych osób i podmiotów.
4) Oprogramowanie umożliwia pracę terminalową poprzez przeglądarkę.
5) Oprogramowanie posiada funkcjonalności zapewniające bezpieczeństwo informacji: posiada wbudowany mechanizm autoryzacji, posiada mechanizmy zabezpieczające przed nieautoryzowanym dostępem.
6) Oprogramowanie umożliwia planowanie audytów z uwzględnieniem audytowanych: lokalizacji, komórek organizacyjnych, wymagań oraz audytorów realizujących audyt i planowanego okresu realizacji audytu.
7) Oprogramowanie udostępnia audytorowi informacje o wymaganiach, które mają zostać poddane audytowi.
8) Oprogramowanie udostępnia audytorowi interfejs do wprowadzania obserwacji audytowych.
9) Oprogramowanie udostępnia audytorowi interfejs do dodawania dowodów audytowych

[7] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 r. poz. 1560 z późn. zm., rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. 2018 poz. 2180), rozporządzanie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. 2018 poz. 2080), rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych oraz rekomendacji CSIOZ/CEZ.

10) Oprogramowanie umożliwia planowanie działań koniecznych do podjęcia wobec obserwacji audytowych zapisanych przez audytora.
11) Oprogramowanie umożliwia przypisanie osób odpowiedzialnych do działań koniecznych do podjęcia wobec obserwacji audytowych zapisanych przez audytora.
12) Oprogramowanie umożliwia przypisanie czasu realizacji do działań koniecznych do podjęcia wobec obserwacji audytowych zapisanych przez audytora.
13) Oprogramowanie udostępnia interfejs do wprowadzania informacji o realizacji działań koniecznych do podjęcia wobec obserwacji audytowych zapisanych przez audytora.
14) Oprogramowanie umożliwia automatyczne generowanie raportów z audytów.
15) Oprogramowanie umożliwia wyświetlanie zadań na tablicy kanban i w formie listy.
16) Oprogramowanie wysyła powiadomienia na adres e-mail użytkownika.
17) Oprogramowanie umożliwia raportowanie postępów realizacji audytu.
18) Oprogramowanie umożliwia podgląd postępów w realizacji audytu.
19) Oprogramowanie wysyła powiadomienie ostrzegawcze (alert) na e-mail użytkownika na podstawie określonych reguł.
20) Obsługa oprogramowania w czasie zbliżonym do rzeczywistego.

6. Oprogramowanie do monitorowania systemów teleinformatycznych wykorzystywanych do świadczenia eUsług z funkcją korelacji zdarzeń bezpieczeństwa o funkcjonalnościach:

1) Oprogramowanie musi dostarczone w formule SaaS na czas świadczenia usługi w ramach umowy.
2) Oprogramowanie jest zgodne z adekwatnymi przepisami prawa[8] oraz w okresie wsparcia dostawcy gwarantuje stałą, pełną zgodność wszelkich realizowanych funkcji/algorytmów rozliczeń/formatów sprawozdań z obowiązującym prawem,
3) Oprogramowanie jest własnością oferenta lub ma prawo do udzielenia licencji i nie narusza praw licencyjnych innych osób i podmiotów.
4) Oprogramowanie umożliwia pracę terminalową poprzez przeglądarkę.
5) Oprogramowanie posiada funkcjonalności zapewniające bezpieczeństwo informacji: posiada wbudowany mechanizm autoryzacji, posiada mechanizmy zabezpieczające przed nieautoryzowanym dostępem.
6) Oprogramowanie umożliwia monitorowanie stanów i zmian parametrów podstawowych systemów wykorzystywanych w zbudowanej infrastrukturze teleinformatycznej wykorzystywanej na potrzeby eUsług.
7) Oprogramowanie umożliwia stworzenie reguł bezpieczeństwa dla dedykowanych i najbardziej prawdopodobnych scenariuszy i wektorów ataków.
8) Oprogramowanie zapewnia udostępnienie danych innym systemom i dedykowanym odbiorcom z wykorzystaniem komunikacji email.
9) Umożliwia monitorowanie i analizę systemów oraz zdarzeń w sieci teleinformatycznej (5 urządzeń, 400 zdarzeń na sekundę).

[8] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 r. poz. 1560 z późn. zm., rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. 2018 poz. 2180), rozporządzanie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. 2018 poz. 2080), rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych oraz rekomendacji CSIOZ/CEZ.

10) Umożliwia korelację danych między różnymi systemami i realizacja założonych scenariuszy (min. 25 reguł korelacji).
11) Umożliwia generowanie alarmów na podstawie określonych reguł.
12) Oprogramowanie wysyła powiadomienie ostrzegawcze (alert) na adres e-mail użytkownika na podstawie określonych reguł.
13) Możliwość wyświetlania szczegółowych informacji o danych zdarzeniach.
14) Obsługa oprogramowania w czasie zbliżonym do rzeczywistego.

Gwarancja i wsparcie oprogramowania:

Min. 24 miesiące gwarancji oraz wsparcia dostawcy usługi
Wykonawca zobowiązany jest w trakcie trwania umowy licencyjnej (wsparcie dostawcy usługi – równe zaoferowanemu terminowi gwarancji, min. 24 miesiące):

1) Dostarczać Zamawiającemu nowsze wersje oprogramowania, uaktualnienia oraz „support packi", poprzez wskazanie miejsca do pobrania i przesłania informacji drogą mailową, wraz z instrukcją instalacji i listą zmian – release notes;
2) Świadczyć usługi opieki serwisowej oraz wsparcia oprogramowania, także na nowszych wersjach oprogramowania – dostarczonych w ramach umowy;
3) Udzielić wsparcia w trakcie instalacji dokonywanych przez Zamawiającego dostarczonego oprogramowania oraz poprawek;
4) Zapewnić rozwiązywanie problemów związanych z instalacją i funkcjonowaniem dostarczonego oprogramowania;
5) Zapewnić przyjmowanie zgłoszeń telefonicznych potwierdzanych zgłoszeniem elektronicznym (www lub e-mail) w trybie 24x7x365 od Zamawiającego z zachowaniem minimalnych warunków przyjęcia zgłoszenia, przez Wykonawcę, tj.:
    - w godzinach pomiędzy 08:00 a 16.00 dnia roboczego – zgłoszenie traktowane jest jak przyjęte danego dnia roboczego;
    - w godzinach pomiędzy 16.00 a 24.00 dnia roboczego – zgłoszenie traktowane jest jak przyjęte o godz. 8.00 następnego dnia roboczego;
    - w godzinach pomiędzy 0.00 a 8.00 dnia roboczego - zgłoszenie traktowane jest jak przyjęte o godz. 8.00 danego dnia roboczego;
    - w dniu ustawowo lub dodatkowo wolnym od pracy - zgłoszenie traktowane jest jak przyjęte o godz. 8.00 najbliższego dnia roboczego;
    - Nie później niż w ciągu 30 minut od momentu otrzymania zgłoszenia awarii potwierdzić przyjęcie zgłoszenia;
6) Zapewnić czas reakcji na zgłoszone problemy, rozumiany jako przesłanie szczegółowego planu działania naprawczego Wykonawcy w związku z dokonanym zgłoszeniem przy zgłoszeniu:
    - błędu krytycznego do 12 godzin od momentu zgłoszenia,
    - błędu niekrytycznego naprawa powinna nastąpić w najbliższym wydaniu oprogramowania.
    - status zgłoszenia określa Zamawiający, wg poniższych kryteriów:
    - błąd krytyczny – nie można otworzyć oprogramowania lub oprogramowanie nie reaguje na polecenia lub samoczynnie zamyka się lub nie działają podstawowe funkcjonalności;
    - błąd niekrytyczny – pozostałe błędy;
7) Zapewnić dostęp do bazy wiedzy o dostarczonym oprogramowaniu;

8) Zapewnić e-mail'owe i telefoniczne konsultacje w zakresie dostarczonego oprogramowania we wszystkie dni robocze w godz. 9.00 – 17.00.

Stacja kliencka

Zamawiający zapewnia stację kliencką z dostępem do Internetu z aktualną wersją przeglądarki internetowej z włączoną obsługą Java Script.

RÓWNOWAŻNOŚĆ:

Norm

Jako normę równoważną normie ISO/IEC 27001:2013 zamawiający dopuszcza inne międzynarodowe normy standaryzujące systemy zarządzania bezpieczeństwem informacji.

Jako normę równoważną normie ISO/IEC 27701:2019 zamawiający dopuszcza inne międzynarodowe normy standaryzujące zarządzanie informacją o prywatności.

Jako normę równoważną normie ISO/IEC 27017 zamawiający dopuszcza inne międzynarodowe normy standaryzujące środki zabezpieczeń informacji dla klientów oraz dostawców usług w chmurze.

Jako normę równoważną normie ISO/IEC 27018 zamawiający dopuszcza inne międzynarodowe normy standaryzujące praktyczne zasady ochrony danych indentyfikujących osobę w chmurze publicznej.

Jako normę równoważną normie PN-EN ISO 22301 zamawiający dopuszcza inne międzynarodowe normy standaryzujące bezpieczeństwo powszechne – systemy zarządzania ciągłością działania.

Jako normę równoważną normie EN 50600 zamawiający dopuszcza inne międzynarodowe normy standaryzujące zagadnienia wyposażenia i infrastruktury centrów przetwarzania danych, z zastrzeżeniem spełniania co najmniej wymogów analogicznych do określonych dla klasy 3 w zakresie wyposażenia i infrastruktury – systemy zabezpieczeń.

Certyfikatów

Jako certyfikaty równoważne do wymaganych dla osoby pełniącej funkcję Koordynatora Testów Bezpieczeństwa oraz osób pełniących funkcję audytora zamawiający dopuszcza analogiczne co do zakresu wskazanych certyfikatów, co jest rozumiane jako (łącznie):

a) analogiczna dziedzina merytoryczna wynikająca z wiedzy, której dotyczy certyfikat (np. kompetencje związane z audytem spełniania określonych norm lub norm równoważnych, wskazanych powyżej),

b) analogiczny stopień poziomu kompetencji (np. podstawowy, zaawansowany, ekspert) wymagany do otrzymania certyfikatu (np. certyfikatu audytora wiodącego dla danej normy lub normy równoważnej wskazanej wyżej, certyfikatu CEH, certyfikatu OSCP),
c) analogiczny poziom doświadczenia zawodowego wymagany dla otrzymania danego certyfikatu (np.: konieczność wykazania się uczestnictwem w określonej liczbie audytów, wdrożeń, szkoleń etc.),
d) uzyskanie certyfikatu potwierdzone jest egzaminem.
e) certyfikat równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od Wykonawcy lub należący do tej samej grupy kapitałowej co Wykonawca (tj. wymagane jest uzyskanie certyfikatu od podmiotu niezależnego od Wykonawcy).