

OPIS PRZEDMIOTU ZAMÓWIENIA – ZADANIE III

1. Przedmiotem umowy jest zakup i dostawa oprogramowania wraz ze szkoleniem, platformy szkoleniowej oraz usługi wykonania dokumentacji SZBI, audytu KRI i szkolenia w ramach realizacji projektu „Cyberbezpieczne Wodociągi” realizowanego przez Gminny Zakład Gospodarki Komunalnej Trzebnica – ERGO Sp. z o.o.

Niniejsze zamówienie ma na celu podniesienie poziomu cyberbezpieczeństwa aby zapewnić odpowiedni poziom bezpieczeństwa kluczowych usług i zasobów Gminnego Zakładu Gospodarki Komunalnej Trzebnica – ERGO Sp. z o.o.

L.p.	Grupa	Przedmiot zamówienia	Ilość / jednostka miary
1.	Z3-IT/ Z3-KOMP	Oprogramowanie do zarządzania siecią wraz ze szkoleniem	1 szt.
2.	Z3-KOMP	Platforma szkoleniowa	1 szt.
3.	Z3-ORG	Opracowanie, aktualizacja i wdrożenie dokumentacji SZBI	1 szt.
4.	Z3-ORG	Audyt KRI	1 szt.
5.	Z3-KOMP	Szkolenie zakresu cyberbezpieczeństwa	1 szt.

1) Oprogramowanie do zarządzania siecią wraz ze szkoleniem

Minimalne wymagania
<p>Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych oraz monitorowania infrastruktury informatycznej spełniające następujące funkcjonalności:</p> <p>1. Oprogramowanie powinno posiadać budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS 1.2.</p> <p>Moduły mają umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych</p>

i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwany użytkownikiem. Program musi wykorzystywać silnik bazy danych nie objęty limitem ilości danych, niewymagającym dodatkowego licencjonowania. Serwer oraz Konsola zarządzająca powinna działać na 64-bitowym systemie operacyjnym Windows.

Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., powinny być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Powinny być również grupowane w osobnym, dedykowanym oknie. Tak aby pozwalała to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.

Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, powinien być objęty kontrolą na poziomie wybranych Administratorów – w programie powinno się nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak

i użytkowników. Główny Administrator powinien mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do opcji programu oraz logów działań innych administratorów. Działania administratorów muszą być logowane oznacza to, że program musi posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog.

Program musi umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityki powinny pozwalać na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymusza dostosowanie bieżących haseł do obowiązujących zasad.

Program musi zawierać mechanizmy uwierzytelniania logowań administratorów do konsoli

z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA powinno się skonfigurować okres, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania może być pominięta tylko w lokalnej konsoli serwera.

2. W ZAKRESIE MONITOROWANIA INFRASTRUKTURY (BEZAGENTOWO) funkcjonalność musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku.
- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze.
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie.
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny.
- zablokowania mapy urządzeń przed przypadkową edycją.
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów.
- serwerów pocztowych:

- program musi monitorować e czas logowania do serwisu odbierającego oraz czas

wysyłania poczty,

- program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),
 - program powinien mieć możliwość wykonywania operacji testowych,
 - program powinien mieć możliwość wystania powiadomienia jeśli serwer pocztowy nie działa.
- monitorowania serwerów WWW i adresów URL.
 - cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS.
 - obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
 - obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID.
 - obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych.
 - monitoringu routerów i przełączników wg:
 - zmian stanu interfejsów sieciowych,
 - ruchu sieciowego,
 - podłączonych stacji roboczych – graficzna prezentacja panelu switcha,
 - ruchu generowanego przez podłączone do portów stacje robocze.
 - serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie.
 - wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu.
 - Monitorowanie stanu maszyn wirtualnych.
 - Zarządzanie stanem maszyn wirtualnych.

- wydajności systemów Windows:
 - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

Program musi posiadać Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Program musi posiadać również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.

Program musi posiadać również definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie m.in.: wysłanie komunikatu pulpitu, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane powinny być przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wykazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.

Program musi umożliwiać nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie. m.in.: wysłanie komunikatu pulpitu, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy powinny być budowane przez administratora z wykorzystaniem ciągu przyczynowo skutkowego — oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Alarmy muszą pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie powinno umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail autoryzacji OAuth 2.0.

Program musi mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

3. W ZAKRESIE INWENTARYZACJI program automatycznie powinien gromadzić informacje o sprzęcie

i oprogramowaniu stacji roboczych oraz:

1. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
3. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
4. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
5. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera.
6. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
7. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
8. Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontaktach lokalnych użytkowników, harmonogramie zadań itp.
9. Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
10. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji muszą być logowane.

Moduł inwentaryzacji zasobów ma umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

- przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
- tworzenie powiązań między zasobami a urządzeniami,
- tworzenie powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- wskazanie osób uprawnionych do użycia zasobów,
- definiowanie własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości,
- dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
- określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importowanie danych z zewnętrznego źródła (.CSV),
- przechowywanie dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
- tworzenie powiązań między zasobami a dokumentami w relacji 1:N,
- oznaczanie statusów zasobów, np. w użyciu, w naprawie, zutilizowany itp.,
- ewidencjonowanie czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,

- generowanie zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- generowanie protokołów przekazania zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- archiwizacje i porównywanie audytów zasobów,
- tworzenie kodów kreskowych dla zasobów,
- drukowanie kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- inwentaryzacje zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android
- inwentaryzacje stacji roboczych niepodłączonych do sieci (bez instalacji Agentu poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowanie alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data”
z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

Dodatkowo dostępny powinien być Agent inwentaryzacji na system Android.

Inwentaryzacja oprogramowania ma zapewniać funkcjonalność w zakresie pozyskiwania informacji

o oprogramowaniu i audycie licencji poprzez:

1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
2. Informacje o aplikacjach używanych w organizacji.
3. Tworzenie własnych wzorców aplikacji.

4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
 5. Informacje o komputerach, na których aplikacja została wykryta.
 6. Zarządzanie posiadanymi licencjami.
 7. Wskazywanie osób odpowiedzialnych za licencję.
 8. Wskazanie użytkowników licencji.
 9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
 10. Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
 11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
 12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.
 13. Możliwość przypisania do programów numerów seryjnych, wartości itp.
- Okna audytowe mają posiadać możliwość filtrowania elementów per oddział.

4. W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program ma umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

- Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
- Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
- Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
- Informacji o edytowanych przez użytkownika dokumentach,

- Historii pracy (cykliczne zrzuty ekranowe),
- Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
- Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
- Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
- Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program ponadto posiada możliwość:

- blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
- blokowania ruchu na wskazanych portach TCP/IP,
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- wykrywania podejrzanej aktywności, wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności, automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności,
- integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT, skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia, automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.

- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,
- przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Program ma mieć możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.

Powinien posiadać wbudowany mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone mają być dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.

Program musi posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

5. PROGRAM MUSI UMOŻLIWIAĆ REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM.

W ramach kontroli stacji użytkownika dostępny musi być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połączenie i opcję odrzucenia takiego połączenia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika.

W niniejszym module musi się znajdować baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Moduł musi umożliwiać również przetwarzanie zgłoszeń w

trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawierać dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością musi być umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł ten musi zawierać również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program ma umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łącami do artykułów w bazie wiedzy. Funkcjonalność modułu ma umożliwiać również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.

Moduł pomocy zdalnej musi umożliwiać również:

- pobieranie listy użytkowników z Active Directory,
- zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
- zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
- zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,
- tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
- automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,

- procesowanie zgłoszeń użytkowników z wiadomości e-mail,
- tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
- wykonywanie operacji na wielu zgłoszeniach równocześnie,
- dołączanie załączników do zgłoszeń,
- rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
- szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
- wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
- zrzuty ekranowe (podgląd pulpitu),
- dystrybucję oprogramowania przez Agenty,
- dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
- zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecenia operacji następuje kolejowanie zadania dystrybucji pliku,
- możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
- planowanie nieobecności pracowników helpdesk,
- obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
- generowanie raportów obsługi helpdesk,
- zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
- zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
- wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.

6.W ZAKRESIE MOŻLIWOŚCI OCHRONY DANYCH PRZED WYCIEKIEM poprzez blokowanie urządzeń.

1. Blokowanie urządzeń i nośników danych.

Program ma mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.

2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskiek.

3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.

4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.

5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.

6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.

7. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender

8. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.

9. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

10.

Zarządzanie prawami dostępu do urządzeń:

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp.

- urządzenia prywatne są blokowane.

3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.

4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.

5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
2. Podłączenie/odłączenie urządzenia przenośnego.

Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

Licencja na 40 stacji roboczych

7. Szkolenie

Szkolenie dotyczące w/w oprogramowania umożliwiającego monitorowanie infrastruktury informatycznej, monitorowanie bezpieczeństwa sieci i użytkowników, zarządzanie zasobami IT oraz aktywami podlegającymi ochronie. Szkolenie jest wskazane by w pełni wykorzystać możliwości zakupionego komponentu bezpieczeństwa. Szkolenie musi być skierowane dla zaawansowanych administratorów sieci. Pozwoli to na poprawne skonfigurowanie poszczególnych modułów oprogramowania oraz wykorzystać w 100% jego funkcjonalności tak aby zapewnić jak najwyższy poziom cyberbezpieczeństwa. Minimum jednodniowe certyfikowane szkolenie w formie warsztatów. Szkolenie dla 2 użytkowników (administratorów).

2) Platforma szkoleniowa

Minimalne wymagania

Zakup dwuletniej subskrypcji platformy szkoleniowej kształtującej dobre praktyki

bezpiecznej pracy w świecie cyfrowym spełniające następujące funkcjonalności:

Platforma ma dostarczać narzędzia i zasoby niezbędne do zapewnienia pracownikom wartościowej wiedzy i umiejętności w zakresie ochrony przed cyberzagrożeniami.

Użytkownicy otrzymują dostęp do materiałów szkoleniowych oraz testów wiedzy.

Menedżerowie grup oraz administratorzy zyskują wgląd w postęp nauki i poziom wiedzy w całej organizacji i dla poszczególnych grup.

Architektura Platformy:

Platforma udostępniania w formie subskrypcji na dostępu do usługi on-line w chmurze.

Zawartość:

Platforma powinna zawierać minimum:

- min. 25 lekcji i 3 testy wiedzy z zakresu podstaw RODO;
- min. 65 lekcji i 15 testów z zakresu cyberbezpieczeństwa dostosowanych do polskich warunków;
- materiały szkoleniowe podzielone na moduły;
- możliwość dostosowywania tempa nauki do potrzeb organizacji, wysyłanie monitów;
- możliwość prowadzenia statystyk i raportów dla użytkowników, grup i kadry kierowniczej;

Platforma powinna być stale rozwijana pod kątem funkcjonalnym oraz zwiększaniem bazy wiedzy szkoleniowej. Należy aby baza szkoleniowa została przygotowana i odpowiednio ułożona przez ekspertów w dziedzinie cyberbezpieczeństwa oraz ochrony danych osobowych, a informacje w niej zawarte mają być są aktualne, istotne i odnoszące się do realnych zagrożeń, na które użytkownik może natknąć się podczas codziennego korzystania z komputera w pracy.

Zakres tematyczny powinien zawierać min. tematy z obszaru:

- RODO wstęp;
- Incydenty i naruszenia ochrony danych;
- RODO – w przykładach i praktyce stosowania;
- Powierzenie przetwarzania danych i wybór dostawcy;
- Socjotechniki;
- Bezpieczeństwo haseł;
- Bezpieczeństwo poczty e-mail i ochrona przed SCAM-em;
- Obrona przed phishingiem;
- Bezpieczeństwo stron WWW i przeglądarek;
- Ataki socjotechniczne z wykorzystaniem urządzeń;
- Ataki za pośrednictwem telefonu;
- Zagrożenia związane z urządzeniami mobilnymi;
- Zagrożenia związane z sieciami Wi-Fi;
- Zagrożenia w mediach społecznościowych;
- Dobre praktyki bezpieczeństwa;
- Prywatność, poufność i anonimowość w Internecie;

Minimalne cechy szkolenia:

- ma umożliwiać monitorowanie postępu użytkownika;
- musi posiadać statusy dla lekcji: nierozpoczęta, w toku, ukończona;
- musi posiadać statusy dla modułu: nierozpoczęty, w toku, ukończony;
- musi posiadać statusy dla testu: nierozpoczęty, rozpoczęty, niezaliczony, zaliczony;

- powinien być brak ustalonej kolejności kursu, użytkownik może od razu przejść do zaliczenia testu lub
- zapoznawać się z lekcjami video według uznania lub według narzuconego w Jednostce harmonogramu;
- Każdy moduł powinien zawierać krótkie streszczenie zawartości;
- Każda lekcja powinna zawierać notatki w formie tekstowej;
- Po ukończeniu materiału użytkownik powinien mieć do niego nieograniczony dostęp w ramach trwającej subskrypcji;;
- Postęp w lekcji powinien być zapisywany, użytkownik po powrocie do danej lekcji zaczyna od momentu, w którym zakończył oglądanie materiału video;
- Kurs ma umożliwiać filtrowanie dostępnych modułów kursu (wszystkie moduły, nowe, rozpoczęte, ukończone);
- Kurs ma pozwalać użytkownikowi na ukrywanie ukończonych lekcji;
- Po ukończeniu kursu użytkownik ma mieć możliwość otrzymania certyfikatu (do wydruku);
- Platforma powinna być dostępna również w wersji mobilnej z poziomu przeglądarki, bez konieczności instalacji dodatkowego oprogramowania;

Minimalne cechy testów:

- Musi składać się z pytań i odpowiedzi jednokrotnego wyboru;
- Do testu można podejść przed ukończeniem lekcji video (dowolna kolejność wykonywania

działań w obrębie kursu);

- Administrator platformy ma mieć możliwość konfigurowania progu punktowego wymaganego do zaliczenia testu;
- Administrator platformy ma możliwość konfigurowania czasu, który musi upłynąć zanim użytkownik po raz kolejny może podejść do testu;
- Test powinien zapamiętywać odpowiedzi użytkownika (na wypadek opuszczenia testu przed ukończeniem);
- Kolejność pytań i odpowiedzi powinna być losowana przed rozpoczęciem przez użytkownika testu;
- Ukończenie/Zaliczenie testu wpływa na postęp ukończenia modułu;
- Nie powinno być limitu czasowego na ukończenie testu;
- Zmiana wymaganego w organizacji progu procentowego zaliczenia testu po ukończeniu przez użytkownika testu nie ma wpływu na status testu (zaliczony/niezaliczony);
- Kurs musi zawierać test końcowy sprawdzający wiedzę z całego kursu;

Zarządzanie platformą przez Spółkę:

- Platforma powinna posiadać specjalne konto Administratora do zarządzania subskrypcją i platformą;
- Konto Administratora głównego nie powinno wliczać się do limitu użytkowników i ma mieć dostęp do wszystkich funkcji platformy;
- Powinny występować jeszcze dwie role: Administratora zwykłego oraz Użytkownika;
- Administrator zwykły ma mieć możliwość zarządzania platformą i dostęp do wszystkich

funkcji platformy;

- Użytkownik powinien mieć jedynie dostęp do swojego konta, pulpitu oraz zawartości szkoleń;
- platforma powinna pozwalać na nadania funkcji menedżera grupy, który zarządza grupa użytkowników (wglądu do ich danych, postępów w nauce itd.)
- platforma powinna posiadać dla menadżerów grup i Administratorów funkcjonalność śledzenia postępów użytkowników w kursach;
- Platforma ma wyświetlać listę aktywności każdego użytkownika wraz z informacją o dacie i rodzaju aktywności;
- Musi posiadać możliwość masowego dodawania i aktualizacji użytkowników do platformy, min. import pliku csv;
- Po dodaniu użytkownika do platformy, otrzymuje on wiadomość e-mail z i ustaleniem pierwszego hasła;
- Administrator może dowolnie dodawać, modyfikować i usuwać użytkowników;
- Administrator może dowolnie oraz dezaktywować konta wszystkich użytkowników;
- Menadżer ma posiadać rozszerzony dostęp do grup i użytkowników, którymi zarządza;
- Administrator może dowolnie tworzyć, edytować oraz usuwać grupy;
- Użytkownik może należeć do dowolnej liczby grup;
- Menedżer nie musi być członkiem grupy, którą zarządza;

Inne możliwości konfiguracyjne i informacyjne platformy:

- Konfiguracja procentowego progu zdawalności testu;
- Konfiguracja czasu przed kolejnym podejściem do testu;
- Konfiguracja minimalnego wymaganego postępu w kursie (liczba ukończonych materiałów na tydzień);

- Informacja o rodzaju subskrypcji;
- Informacja o czasie pozostałym do wygaśnięcia subskrypcji;
- Wykres limitu użytkowników (użytkownicy w Jednostce/limit subskrypcji);
- Platforma powinna posiadać dedykowaną i stale aktualizowaną Bazę Wiedzy, w której znajdują się artykuły objaśniające najważniejsze funkcje platformy;
- Platforma powinna posiadać funkcjonalność newslettera wysyłany na adres e-mail użytkowników;

Zarządzanie treścią:

- Platforma musi pozwalać na globalne włączanie lub wyłączanie materiałów edukacyjnych;
- Platforma musi pozwalać na nieograniczone dodawanie własnych materiałów;
- wymagana jest możliwość podejrzenia postępu nauki w konkretnym materiale edukacyjnym użytkowników w organizacji;

Inne:

- platforma powinna wspierać przeglądarki min. (Google Chrome, Mozilla Firefox, Microsoft Edge)
- powinna być możliwość przedłużenia subskrypcji oraz zwiększenia limitu użytkowników w ramach istniejącej subskrypcji.

Licencja na 40 użytkowników

3) Opracowanie, aktualizacja i wdrożenie dokumentacji SZBI

Minimalne wymagania
Opracowanie i wdrożenie dokumentacji SZBI, analizy ryzyka i planów ciągłości działania spełniającego wymagania norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji

(w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005) oraz ISO 31000 w zakresie zarządzania ryzykiem, oraz Systemu Zarządzania Ciągłością Działania – w zakresie systemów teleinformatycznych. Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb Spółki dokumentację SZBI z wymaganiami powołanych wyżej norm. Opracowane polityki, procedury itd. muszą realnie odnosić się do procesów w Spółce. Celem wdrożenia jest zapewnienie wysokiego poziomu bezpieczeństwa informacji i spełnienie wymagań:

- rozporządzenia 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.
- ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
- Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (tzw. Dyrektywa NIS 2).

Usługę można przeprowadzić w formie hybrydowej (w siedzibie Spółki oraz zdalnie) gdzie na realizację należy przeznaczyć minimum 3 dni.

W ramach usługi przygotowane i wdrożone zostaną:

1. Audyt środowiska jednostki, obejmujący aktualną strukturę organizacyjną i realizowane procesy oraz wymagania prawne ich funkcjonowania.

2. Przegląd aktualnej dokumentacji bezpieczeństwa informacji (jeśli istnieje) , w tym polityk, procedur, instrukcji, regulaminów, wytycznych.

3. Inwentaryzację i analizę aktywów - zasobów informacyjnych oraz środków służących do gromadzenia i przetwarzania informacji.

4. Przygotowanie i wdrożenie dokumentacji SZBI

W ramach usługi przygotowane i wdrożone zostaną dokumenty będące elementem Systemu Zarządzania Bezpieczeństwem Informacji wymagane w rozporządzeniu KRI tj.:

- a. Polityka Bezpieczeństwa Teleinformatycznego
- Zasady korzystania z systemów informatycznych,
 - Procedura zmiany uprawnień,
 - Instrukcja wykonywania kopii zapasowej,

- Instrukcja odtworzenia kopii zapasowej,
- Rejestr komponentów bez wsparcia producentów,
- Protokół przekazania sprzętu do naprawy,
- Zarządzanie konfiguracją, - Wzorce konfiguracji,
- Rejestr komponentów środowiska teleinformatycznego,
- Lista parametrów wydajności i pojemności,
- Zapisy do raportów monitorowania wydajności i pojemności,
- Zapisy do raportów monitorowania usług zewnętrznych,
- Instrukcja wycofania komponentów teleinformatycznych.
- Zasady prowadzenia audytu wewnętrznego systemów teleinformatycznych.
- Procedury monitorowania i przeglądu systemów teleinformatycznych.
- Zasady wprowadzania i wyprowadzania danych do systemów teleinformatycznych
- Zasady szkolenia użytkowników systemów teleinformatycznych

b. Polityka Bezpieczeństwa Informacji

- Deklaracja stosowania,
- Rejestr definicji,
- Przypisanie odpowiedzialności i ról w zakresie utrzymywania SZBI,
- Polityka Klasyfikacji Informacji,
- Polityka Klasyfikacji Systemów Informatycznych,
- Opis metodyki szacowania ryzyka,
- Raport z procesu szacowania ryzyka,
- Plan postępowania z ryzykiem,
- Monitorowanie i przegląd SZBI.
- Zasady zarządzania incydentami bezpieczeństwa,
- Zasady zarządzania rejestrem wyjątków od PBI.
- Odwołania do innych aktów wewnętrznych Zamawiającego.

c. Zarządzanie dostawcami usług informatycznych

- Wzory klauzul do umów z dostawcami,
- Przykładowe porozumienie o poufności,
- Zasady zwrotu informacji,
- Rejestr umów zawartych z dostawcami zewnętrznymi,
- Przegląd umowy i ocena dostawcy usługi.

d. Opracowanie i przekazanie zamawiającemu na podstawie protokołu odbioru kompletnej dokumentacji SZBI (wszystkich wymaganych przez powołane normy polityk, planów, procedur, instrukcji, metodologii zarządzania ryzykiem itd.)

5. Przygotowanie Analizy Ryzyka

- a. Przeprowadzenie przy udziale przedstawicieli Zamawiającego i udokumentowanie analizy ryzyka, w tym opracowanie i wdrożenie metodyk:**
- dokonanie oceny zabezpieczeń technicznych i organizacyjnych stosowanych przez Zamawiającego;

- opracowanie raportu bezpieczeństwa na podstawie przeprowadzonej oceny stosowanych przez Zamawiającego zabezpieczeń technicznych i organizacyjnych;
- identyfikacja ryzyk w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji, w tym ochrony danych osobowych;
- ocena ryzyk;
- wykonanie DPIA – oceny skutków dla ochrony danych osobowych przetwarzanych przez Zamawiającego;
- przygotowanie planów postępowania z ryzykiem.

b. Wskazanie obszarów wymagających dostosowania i/lub doskonalenia adekwatnie do przeprowadzonej analizy ryzyka oraz wymagane do wdrożenia zabezpieczenia.

6. Przygotowanie i wdrożenie Planów Ciągłości Działania (PCD)

a. Przygotowanie i planowanie:

- szkolenia/warsztaty dla osób odpowiedzialnych za nadzorowanie,
- Identyfikacja kluczowych procesów,
- Inwentaryzacja kluczowych zasobów dla każdego procesu,
- Przeprowadzenie analizy wpływu na biznes (BIA),
- Analiza wymagań organizacji, klientów, regulacyjnych,
- Określenie RPO (recovery point objective) maksymalna ilość utraty danych określona w czasie,
- Określenie RTO (recovery time objective) określenie czasu, po którym zostanie wznowiona usługa/proces.

W efekcie należy wypracować listę procesów krytycznych i czasów RPO i RTO oraz listę zasobów.

b. Polityka zapewnienia ciągłości działania.

- adaptacja polityki przez zespół ds. ciągłości działania,
- określenie kontekstu i identyfikacja procesów, które zostaną objęte PCD oraz ich klasyfikacja na podstawie BIA,
- wskazanie i analiza podmiotów realizujących zadania niezbędne do zapewnienia ciągłości działania,
- wskazanie i analiza zasobów niezbędnych do realizacji procesu w trybie odtwarzania ciągłości,
- określenie ryzyk wpływających na zapewnienie ciągłości działania.

W efekcie należy wypracować Politykę Ciągłości Działania, Analizę ryzyka, inwentaryzację i klasyfikację procesów.

c. Implementacja i działanie.

- przypisanie obowiązków personelowi i zapewnienie kompetencji personelowi,
- mechanizmy komunikacji (z pracownikami, podmiotami, klientami i mediami),
- przygotowanie procedur odtwarzania środowiska teleinformatycznego (BCP business continuity plans) w tym instrukcji odtworzeniowych (odtworzenie serwerów, urządzeń wirtualnych, instrukcja przełączenia)
- zapewnienie dostępu do niezbędnej dokumentacji odtworzeniowej,
- zarządzanie incydentami,
- wdrożenie procesu detekcji i monitorowania zdarzeń,
- powrót do pracy normalnej.

W efekcie należy wypracować *Dokumentację MAK dla jednego krytycznego procesu, instrukcje odtworzeniowe, wdrożony proces zarządzania incydentami.*

d. Ocena pracy.

- Weryfikacja aktualności planów,
 - Testowanie przyjętych scenariuszy, testowanie planów, weryfikacja instrukcji odtworzeniowych oraz wykonanie raportu z testów.
 - Mierzenie skuteczności przyjętych planów,
 - Audyt przyjętych planów postępowania z ryzykiem.
- W efekcie należy wypracować raport audytowy.

4) Audyt KRI

Minimalne wymagania

Przeprowadzenie audytu systemu bezpieczeństwa informacji.

Zakres audytu musi być zgodny z kryteriami zawartymi w § 20 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-ISO/IEC 27001

Audyt musi być przeprowadzony przez audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999).

Audyt można przeprowadzić w formie hybrydowej (w siedzibie Spółki oraz zdalnie) gdzie na realizację należy przeznaczyć minimum 3 dni.

Audyt Wiodący. Wymagany ważny do końca projektu certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji Wg normy PN-EN ISO/IEC 27001:2023-08. Doświadczenie Wykonawcy potwierdzone referencjami. Doświadczenie zawodowe audytora wiodącego stanowi pozacenowe kryterium oceny ofert. Oferta otrzyma punkty za liczbę opracowanych kompletnych audytów KRI.

Audyt zgodności z wymaganiami Krajowych Ram Interoperacyjności

Celem audytu jest usługa, która polega na przeprowadzeniu analizy i oceny stopnia przygotowania do spełnienia wymagań stawianych przez KRI. Audyt ma pomóc prawidłowo przygotować się do wdrożenia wymagań stawianych przez KRI. Zwrócić należy uwagę na aspekty, które należy poprawić i działania jakie należy bezwzględnie podjąć, aby sprostać wymogom określonym w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności.

Należy przyjąć wzorcowy harmonogram:

- Weryfikacja dokumentacji,
- Weryfikacja analizy ryzyka,
- weryfikacja procedur organizacyjnych,
- Weryfikacja planów ciągłości działania,
- Weryfikacja WCAG,
- Kontrola zabezpieczeń technicznych,
- Końcowy raport audytu.

Zakres zadań do zrealizowania:

a. Weryfikacja dokumentacji

Kontrolą objęte są wymagane dokumenty niezbędne do realizacji zadań stawianych przez

Krajowe Ramy Interoperacyjności.

Minimalny zakres obejmuje:

- zapisy dotyczące zasad bezpiecznego przetwarzania informacji,
- zapisy dotyczące współpracy z dostawcami kluczowych usług,
- zapisy klasyfikacji informacji przetwarzanej w Jednostce,
- zapisy dotyczące udostępniania informacji,
- zapisy dotyczące zarządzania incydentami,
- zapisy monitorowania bezpieczeństwa informacji,
- zapisy dotyczące zarządzaniem oprogramowaniem,
- zapisy dotyczące wykonywanie kopii zapasowej,
- zapisy dotyczące napraw sprzętu,
- zapisy dotyczące utylizacji sprzętu,
- zapisy dotyczące ponownego wykorzystania sprzętu.

b. Weryfikacja analizy ryzyka

Weryfikacja obejmuje minimum:

- poprawność identyfikacji systemów i komponentów do analizy,
- poprawność przeprowadzenia analizy prawdopodobieństwa,
- szacowanie strat,
- ocenę mechanizmów zabezpieczających,
- rejestr zidentyfikowanych ryzyk,
- plan postępowania z ryzykiem.

c. Weryfikacja procedur

Kontrolą należy objąć następujące procesy:

- proces zarządzania uprawnieniami,
- weryfikacja działań na uprawnieniach administratora,
- kontrola aktualności regulacji,
- monitorowanie dostępu do informacji,
- inwentaryzacja sprzętu i oprogramowania,
- kontrola pracy zdalnej i pracy na odległość,
- kontrola zasad postępowania z informacjami,
- monitorowanie zgodności z normami wskazanymi w KRI,
- kontrola zaleceń audytowych,
- proces szkolenia pracowników,
- proces raportowania działań,
- proces utylizacji sprzętu,
- proces udostępniania danych,
- proces zgłaszania incydentów.

d. Weryfikacja Planu Ciągłości Działania

Przebieg identyfikacji powinien uwzględniać:

- weryfikacja strategii utrzymania Planu Ciągłości Działania,
- analiza procedur zapewniających ciągłość działania,
- analiza testów weryfikujących skuteczność przyjętych planów.

e. Kontrola zgodności z WCAG (Web Content Accessibility Guidelines).

Kontrola obejmuje pięć punktów kontrolnych wybranych przez audytora w zależności od treści prezentowanych na stronie internetowej jednostki.

f. Kontrola zabezpieczeń technicznych.

Zakresem kontroli należy objąć weryfikację:

- zabezpieczenia danych przed nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem,
- skuteczności mechanizmów pozwalających na zapewnienie aktualności oprogramowania,
- procedur odtworzeniowych danych z kopii zapasowych,
- mechanizmów zabezpieczających informacje na stronie internetowej jednostki oraz BIP,
- mechanizmów zabezpieczających stosowanych do zabezpieczenia poczty elektronicznej,
- zabezpieczeń połączeń zdalnych,
- zidentyfikowanych mechanizmów kryptograficznych wykorzystywanych w Jednostce,
- zarządzania ryzykiem związanym z opublikowanymi podatnościami technicznymi,
- mechanizmów realizowanych po wykryciu podatności,
- nadzorowania działań wykonywanych na uprawnieniach administratora,
- nadzorowania parametrów środowiskowych w serwerowni,
- uprawnień w systemach informatycznych objętych KRI,
- zapewnienia odpowiedniej jakości haseł,
- zapewnienia bezpieczeństwa nośników przeznaczonych do utylizacji,
- sposobu przechowywania kopii zapasowych,
- monitorowania działań inicjowanych z sieci publicznej.

W efekcie sporządzony musi zostać raport audytowy zawierający:

- ocenę weryfikowanego obszaru,
- opis aktualnego stanu bezpieczeństwa danych osobowych,
- wytyczne, które należy wdrożyć w celu uzyskania pełnej zgodności z wymaganiami ustawy.

5. Szkolenie zakresu cyberbezpieczeństwa

Minimalne wymagania
Jednodniowe podstawowe szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników (15 osób) Agenda szkolenia: 1. Wprowadzenie do tematu Cyberbezpieczeństwa 2. Incydenty bezpieczeństwa w Polsce 3. Wrażliwe dane firmowe - czym są i jak się z nimi obchodzić? Klasyfikacja danych, jakie dane udostępniamy w sieci. 4. Typy zagrożeń. Phishing, Malware, Ransomware - co to jest i w jaki sposób jesteśmy na niego podatni? 5. W jaki sposób dane mogą wyciec z naszej organizacji? 6. Podstawy bezpieczeństwa informatycznego

7. Kiedy powinna zapalić nam się "lampa bezpieczeństwa"?
8. W jaki sposób zabezpieczać i udostępniać firmowe dane?
9. Dlaczego i jak zabezpieczamy dane?
10. Reakcja na incydenty bezpieczeństwa
11. Q&A

Wymagania ogólne dotyczące identyfikacji oferowanego sprzętu oraz zasad równoważności.

1. Dla jednoznacznej identyfikacji oferowanych rozwiązań należy podać co najmniej nazwę producenta, a także nazwę i model oferowanego produktu lub jego oznaczenie kodowe wg. producenta. Zamawiający wymaga określenia oferowanych produktów i faktycznych parametrów, o których mowa w powyższym opisie, w taki sposób, by oceniający byli w stanie stwierdzić, czy zaoferowane rozwiązanie spełnia wymagania specyfikacji. Przedmiotowe informacje są składane na potwierdzenie, iż oferowane rozwiązania spełniają wymagania Zamawiającego. Ciężar wykazania spełnienia przez oferowane rozwiązania wymogów określonych przez Zamawiającego w specyfikacji spoczywa na składającym ofertę.
2. O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
3. W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.
4. W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.
5. Pod pojęciem rozwiązań równoważnych, o ile nie dokonano doprecyzowania w danym zakresie, Zamawiający rozumie taki sprzęt i oprogramowanie, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w Opisie Przedmiotu Zamówienia.
6. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.
7. Ciężar udowodnienia równoważności w stosunku do wymogów określonych przez Zamawiającego spoczywa na składającym ofertę. W takim przypadku Wykonawca musi przedłożyć odpowiednie dokumenty, opisujące parametry techniczne, wymagane prawem certyfikaty i inne dokumenty, dopuszczające dane produkty do użytkowania oraz pozwalające jednoznacznie określić, że są równoważne.



GMINA
TRZEBNICA
trzebnica.pl



GMINNY
ZAKŁAD
GOSPODARKI
KOMUNALNEJ



KRAJOWY
PLAN
ODBUDOWY



Rzeczpospolita
Polska

Sfinansowane przez
Unię Europejską
NextGenerationEU

