**Załącznik nr 1 do zapytania ofertowego**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

*(zamówienie o wartości poniżej kwoty 130 000 złotych realizowane bez stosowania przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych)*

1. **Informacje ogólne dotyczące przedmiotu zamówienia**

Przedmiotem zamówienia jest wykonanie przez Wykonawcę na rzecz Zamawiającego konfiguracji i świadczenie usługi dostępu do systemu do kontroli zarządczej (dalej: „System”) w modelu „Software as a Service” (dalej: „SaaS”) dla Ministerstwa Aktywów Państwowych (dalej: „MAP”), zainstalowanego w chmurze na bezpiecznej infrastrukturze, udzielenie konsultacji przy opracowaniu regulacji dotyczących kontroli zarządczej (dalej: „KZ”) oraz przeprowadzenie szkolenia z KZ dla pracowników MAP.

System ma być narzędziem do realizacji w MAP obowiązku KZ, zgodnie z art. 68 ustawy z dnia 27 sierpnia 2009 r. *o finansach publicznych[[1]](#footnote-1)*, oraz ma wspierać kierownictwo i pracowników MAP w tych działaniach.

Wykonawca zapewni zgodność Systemu z:

1. ustawą *o finansach publicznych*,
2. komunikatem nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. *w sprawie standardów kontroli zarządczej dla sektora finansów publicznych* (dalej jako: standardy KZ),
3. komunikatem nr 3 Ministra Finansów z dnia 16 lutego 2011 r. *w sprawie szczegółowych wytycznych w zakresie samooceny kontroli zarządczej dla jednostek sektora finansów publicznych*,
4. komunikatem nr 6 Ministra Finansów z dnia 6 grudnia 2012 r. *w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania zarządzania ryzykiem*,
5. rozporządzeniem z dnia 29 września 2010 r. Ministra Finansów *w sprawie planu działalności i sprawozdania z jego wykonania[[2]](#footnote-2)*,
6. ustawą z dnia 4 kwietnia 2019 r. *o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych[[3]](#footnote-3)*,
7. ustawą z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne[[4]](#footnote-4)*,
8. ustawą z dnia 10 maja 2018 r. *o ochronie danych osobowych[[5]](#footnote-5)*,
9. ustawą z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne[[6]](#footnote-6),*
10. rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[[7]](#footnote-7)*,
11. rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych* – dalej również: RODO*)[[8]](#footnote-8),*
12. Standardami Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) na Poziomie SCCO2: Kontrolowane informacje urzędowe,
13. rozporządzenie Ministra Finansów z dnia 4 września 2015 r. *w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu*[[9]](#footnote-9),
14. komunikat Ministra Rozwoju i Finansów z 12.12.2016 r. *w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych*[[10]](#footnote-10).
15. **Informacje szczegółowe dotyczące przedmiotu zamówienia**

W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest do:

1. Skonfigurowania Systemu w modelu SaaS zainstalowanego w chmurze na bezpiecznej infrastrukturze dla MAP, w tym:
2. zaimportowania do systemu danych przekazanych przez MAP, w tym struktury organizacyjnej MAP, projektu Planu działalności Ministra na rok 2025, projektów planów komórek organizacyjnych, ankiety z samooceny KZ za rok 2024, projektu sprawozdania z realizacji Planu działalności Ministra za rok 2024,
3. uzupełnienia słowników (bazy danych dotyczących m.in. ryzyk) w zakresie wskazanym przez MAP,
4. założenia kont dla użytkowników i nadania im uprawnień.
5. Udzielenia 24 godzin konsultacji przy opracowaniu ok. 2-3 regulacji wewnętrznych MAP w zakresie KZ pod kątem funkcjonalności systemu.
6. Przeprowadzenia minimum 2,5 godzinnego szkolenia z KZ, w formie on-line, dla pracowników MAP zgodnie z przepisami prawa powszechnie obowiązującego w obszarze KZ, wskazanymi w rozdziale I lit. a-e oraz metodyką zgodną z funkcjonalnościami Systemu.

Tematyka szkolenia powinna obejmować m.in. standardy KZ, planowanie, wyznaczanie celów, mierników i zadań, zarządzanie ryzykiem – analizę i dokumentowanie, monitorowanie KZ. Wykonawca zaproponuje co najmniej po dwa terminy szkolenia dla ok. 400 pracowników MAP dla dwóch grup uczestników: kierownictwa oraz pracowników.

Szkolenie powinno zostać zrealizowane za pośrednictwem profesjonalnej platformy/aplikacji do szkoleń online, przyjęte rozwiązanie teleinformatyczne nie może wymagać instalowania na komputerach uczestników jakichkolwiek płatnych aplikacji. Wykonawca zapewni uczestnikom szkolenia pomoc techniczną przed i w trakcie jego trwania w zakresie rozwiązywania ewentualnych problemów (np. z logowaniem, właściwym odbiorem technicznym, udziałem w czacie itp.). Szkolenie będzie prowadzone „na żywo” w czasie rzeczywistym, z pełnym udźwiękowieniem i prezentacją treści (np. pokaz slajdów, udostępnienie ekranu itp.). Nie dopuszcza się wcześniej nagranego materiału. Wykonawca sporządzi listy obecności z każdego przeprowadzonego szkolenia i przekaże je Zamawiającemu nie później niż w terminie 7 dni od zakończenia szkolenia. Wykonawca wystawi zaświadczenie potwierdzające udział w szkoleniu i przekaże je uczestnikom oraz Zamawiającemu nie później niż w terminie 7 dni od zakończenia szkolenia.

1. Zapewnienia stałego dostępu do Systemu w chmurze wraz z jego utrzymaniem przez okres 24 miesięcy liczony od podpisania przez Zamawiającego bez zastrzeżeń protokołu odbioru usługi, o której mowa w pkt. 1-3. Wykonawca zapewni ciągłość świadczenia usługi oraz odpowiedni poziom cyberbezpieczeństwa i ochrony danych osobowych zgodnie z odpowiednimi przepisami prawa powszechnego, w tym:
2. możliwość pracy około 400 użytkownikom Zamawiającego,
3. instruktaż (w formie on-line lub w siedzibie MAP) dla pracowników MAP w terminie uzgodnionym przez Strony:
4. minimum 3-godzinnego instruktażu dla kadry kierowniczej MAP,
5. minimum 1,5-godzinnego instruktażu dla pracowników MAP,
6. minimum 1,5-godzinnego instruktażu dla administratorów zarządzających Systemem.

Instruktaż powinien obejmować m.in. następujące zagadnienia: logowanie do systemu i informacje techniczne, strukturę systemu, słowniki, wyznaczanie celów strategicznych i operacyjnych, tworzenie planu działalności Ministra i sprawozdania z jego wykonania, tworzenie planu działalności komórki organizacyjnej i sprawozdania z jego wykonania, zarządzanie ryzykiem w systemie i tworzenie raportów, zarządzanie zadaniami w systemie, monitorowanie, wypełnianie ankiet samooceny KZ, komunikację w systemie.

Wykonawca powinien zaproponować co najmniej dwa terminy przeprowadzenia instruktażu.

1. dostosowywanie Systemu do przepisów powszechnie obowiązujących w obszarze KZ. W przypadku zmiany przepisów w zakresie KZ Wykonawca dostosuje System do tych zmian najpóźniej w dniu wejścia ich w życie;
2. webinaria edukacyjne dotyczące nowych funkcjonalności Systemu i zmian Systemu oraz stały dostęp do materiałów e-learningowych umieszczonych na serwerze Wykonawcy lub na serwerach zewnętrznych,
3. asystę techniczną, w tym 10 godzin projektowych zapewniających bieżące funkcjonowanie Systemu,
4. wsparcie techniczne użytkowników Systemu, polegające na rozwiązywaniu problemów technicznych oraz funkcjonalnych, realizowane telefonicznie lub za pośrednictwem środków komunikacji elektronicznej (poczty elektronicznej, Microsoft Teams) w dniach roboczych dla MAP (od poniedziałku do piątku) w godzinach pracy urzędu, z wyłączeniem dni ustawowo wolnych od pracy,
5. utrzymanie Systemu polegające na:
6. usuwaniu błędów:
   1. krytycznych – rozumianych jako nieprawidłowe działanie usługi powodujące albo całkowity brak możliwości korzystania z usługi albo takie ograniczenie możliwości korzystania z niego, że przestaje ono spełniać swoje podstawowe funkcje:
      1. Czas reakcji na błąd krytyczny: 4h
      2. Czas naprawy błędu krytycznego: 48h;
   2. poważnych – rozumianych jako nieprawidłowe działanie usługi powodujące ograniczenie korzystania z usługi przy zachowaniu spełniania przez usługę jego podstawowych funkcji:
      1. Czas reakcji na błąd poważny: 8h
      2. Czas naprawy błędu poważnego: 72h;
   3. niskiej kategorii – rozumianych jako nieprawidłowe działanie usługi niepowodujące ograniczenia korzystania z usługi:

1.Czas reakcji na błąd niskiej kategorii: 16h

2.Czas naprawy błędu niskiej kategorii: 20 dni;

1. przygotowanie i przekazywanie w wersji elektronicznej aktualnej dokumentacji użytkowników oraz technicznej, materiałów instruktażowych sporządzonych w języku polskim, dotyczących działania i zarządzania udostępnianym Systemem przeznaczonych dla administratorów Zamawiającego na adres e-mail [UmowyIT@map.gov.pl](mailto:UmowyIT@map.gov.pl).

Wykonawca jest zobowiązany do realizacji ww. przedmiotu zamówienia w następujących terminach:

* określonego w punktach 1-3 nie później niż do 9 grudnia 2024 r.,
* określonego w punkcie 4 przez cały okres trwania umowy, od dnia podpisania przez Zamawiającego bez zastrzeżeń protokołu odbioru usługi, o której mowa w pkt. 1-3.

Harmonogram realizacji zamówienia będzie stanowił załącznik do oferty Wykonawcy.

1. **Zgodność z RODO**
2. Wykonawca zobowiązuje się do:
3. zawarcia umowy powierzenia przetwarzania danych osobowych. Wzór umowy powierzenia przetwarzania danych osobowych stanowi Załącznik nr 7do Umowy;
4. zapewnienia zgodności Systemu z RODO;
5. nieprzetwarzania danych osobowych (w tym ich przechowywania, kopiowania, przesyłania) znajdujących się w Systemie poza obszarem Unii Europejskiej.
6. W przypadku korzystania przez Wykonawcę z usług podwykonawców – konieczne będzie ich zidentyfikowanie i zapewnienie przez Wykonawcę, że spełniają wymogi OPZ w zakresie bezpieczeństwa informacji i danych, w tym danych osobowych i uzyskanie zgody Zamawiającego na podpowierzenie przetwarzania.
7. W związku z przetwarzaniem danych osobowych Zamawiający powierzy Wykonawcy przetwarzanie danych osobowych, których Zamawiający jest administratorem.
8. **Zaoferowane przez Wykonawcę rozwiązanie musi spełniać minimalne wymagania przedstawione poniżej:**

W systemie mają być dostępne następujące funkcjonalności:

1. PLANOWANIE DZIAŁALNOŚCI

Ma umożliwić co najmniej:

1. planowanie działalności MAP w perspektywie długookresowej (cele strategiczne) i krótkookresowej (cele operacyjne),
2. sporządzanie planu działalności Ministra zgodnie z wymogami rozporządzenia *w sprawie planu działalności i sprawozdania z jego wykonania*;
3. sporządzanie planów komórek organizacyjnych,
4. określanie celów, mierników i zadań do planu działalności Ministra oraz planów komórek organizacyjnych, przy czym do celu można przypisać wiele mierników i zadań, a ich definiowanie powinno być możliwe w ujęciu kaskadowym (tj. możliwe powiązanie celów i zadań z planu działalności Ministra z planami komórek organizacyjnych),
5. akceptowanie celów, mierników, zadań (np. do planu działalności Ministra, planu komórki organizacyjnej), zgodnie z przyjętą ścieżką akceptacji w ramach hierarchii służbowej (np. pracownik-naczelnik- zastępca dyrektora- dyrektor- nadzorujący członek kierownictwa – akceptacja co najmniej 4-poziomowa).
6. ZARZĄDZANIE RYZYKIEM

Ma umożliwić co najmniej:

1. wybór ryzyka z zapewnionej bazy/biblioteki ryzyk i dodawanie nowych ryzyk przez użytkownika,
2. identyfikację ryzyka w odniesieniu do celów i zadań określonych w planie działalności Ministra i w planach komórek organizacyjnych oraz określanie właściciela ryzyka,
3. okresową analizę i ocenę ryzyka w odniesieniu do realizowanych zadań i celów,
4. akceptowanie ryzyk, zgodnie z przyjętą ścieżką akceptacji w ramach hierarchii służbowej (akceptacja co najmniej 4-poziomowa),
5. dostarczanie użytkownikom informacji o ryzykach niezbędnych do wykonywania przez nich zadań,
6. wprowadzenie kategorii/obszarów/grup ryzyk, a następnie ich monitorowanie, filtrowanie i sortowanie według wybranych kategorii, obszarów lub grup (wybór np.: strategiczne, projektów, zadań itd.),
7. dostarczanie kierownictwu informacji o ryzykach,
8. generowanie raportów o ryzykach (w formie graficznej i tabelarycznej, obejmującej etap stwierdzenia wystąpienia ryzyka, jak i etap ich akceptowania) oraz podejmowanie na ich podstawie decyzji zarządczych,
9. powiadamianie wybranych użytkowników e-mailem o wystąpieniu ryzyka nieakceptowalnego,
10. sporządzenie oraz aktualizowanie rejestru ryzyk, co najmniej poprzez dane: kategoria ryzyka (wybór np.: finanse, kadry, operacyjne, medialne, bezpieczeństwo, cyberbezpieczeństwo, zamówienia publiczne, dane osobowe, korupcyjne itd.), obszar ryzyka, nazwa ryzyka, opis ryzyka, prawdopodobieństwo – ocena punktowa, skutek – ocena punktowa, ocena ryzyka (automatyczna ocena powstała z iloczynu prawdopodobieństwa i skutku), poziom (np. akceptowalny/nieakceptowalny), osoba odpowiedzialna za zarządzanie ryzykiem, termin wykonania działań,
11. dokumentowanie zarządzania ryzykiem,
12. zarzadzanie ryzykiem w sposób systemowy począwszy od identyfikacji ryzyka, przez ocenę i określenie sposobu postępowania w rejestrze, do wygenerowania mapy ryzyka.
13. MONITOROWANIE I SPRAWOZDAWCZOŚĆ

Ma umożliwić co najmniej:

1. okresowe monitorowanie stanu realizacji zadań określonych w planie działalności Ministra i w planach komórek organizacyjnych,
2. bieżące monitorowanie realizacji zadań przypisanych poszczególnym komórkom organizacyjnym i wyznaczonym w ich ramach pracownikom,
3. monitorowanie raz w miesiącu stanu realizacji celów operacyjnych i strategicznych określonych w planie działalności Ministra,
4. sporządzanie sprawozdania z wykonania planu działalności Ministra zgodnie z wymogami rozporządzenia *w sprawie planu działalności i sprawozdania z jego wykonania* oraz z planów komórek organizacyjnych,
5. powiadamianie automatyczne użytkowników o zbliżającym się terminie sporządzenia sprawozdania z wykonania planu działalności Ministra,
6. sporządzanie sprawozdania z wykonania planu komórki organizacyjnej,
7. powiadamianie automatyczne użytkowników o zbliżającym się terminie sporządzenia sprawozdania z wykonania planu komórki organizacyjnej,
8. generowanie dokumentacji według standardów KZ,
9. akceptowanie sprawozdań, zgodnie z przyjętą ścieżką akceptacji w ramach hierarchii służbowej (akceptacja co najmniej 4-poziomowa).
10. ANKIETY

Ma umożliwić co najmniej:

1. publikowanie w systemie ankiet, którymi zarządzać może uprawniony użytkownik,
2. opracowywanie ankiet z pytaniami jednokrotnego i wielokrotnego wyboru, a także pytaniami otwartymi,
3. generowanie ankiety samooceny KZ dla różnych grup użytkowników (np.: dla kadry kierowniczej, dla pracowników),
4. anonimowe wypełnianie ankiety samooceny KZ przez użytkowników,
5. powiadamianie automatyczne użytkowników o zbliżającym się terminie wypełnienia ankiety samooceny KZ,
6. przeprowadzanie samooceny KZ za pośrednictwem ankiety,
7. edytowanie odpowiedzi w ankiecie przed jej zatwierdzeniem/wysłaniem oraz zapisywanie aktualnego stanu wypełnienia ankiety w przypadku wyjścia z formularza,
8. generowanie raportu z wyniku samooceny KZ (również graficznych analiz udzielonych odpowiedzi w postaci wykresów), w tym z podziałem na poszczególne komórki organizacyjne,
9. generowanie statystyki wypełniania ankiet w ujęciu procentowym (aktualny stan),
10. ograniczenie dostępu użytkowników do raportów poprzez zarządzanie uprawnieniami.
11. ZARZĄDZANIE ZADANIAMI (W TYM NIEZGODNOŚCIAMI)

Ma umożliwić co najmniej:

1. tworzenie indywidualnych słowników zdarzeń (baz: celów, zadań oraz mierników),
2. grupowanie danych zawartych w słownikach,
3. filtrowanie bazy po zdefiniowanych właściwościach, np. pokazanie tylko zadań z wybranej kategorii lub przypisanych danej komórce organizacyjnej,
4. przypisywanie zadań dla poszczególnych komórek organizacyjnych do celów strategicznych i operacyjnych wraz ze wskazaniem osoby odpowiedzialnej za realizację danego zadania,
5. przypisywanie zadań zlecanych przez kierownictwo Ministerstwa poszczególnym komórkom organizacyjnym/osobom odpowiedzialnym za realizację zlecanego zadania,
6. filtrowanie podglądu stanu realizacji celów/zadań/mierników według zdefiniowanych właściwości (np. kategoria, obszar, priorytet) lub komórek organizacyjnych (np. podgląd celów i zadań z wybranej kategorii),
7. zgłaszanie przez użytkowników incydentów (zdarzeń związanych z wystąpieniem niezgodności),
8. prowadzenie rejestru incydentów (niezgodności),
9. wyznaczanie zadań doskonalących i naprawczych,
10. archiwizacja (usunięcie z bazy) celów/zadań/mierników z zachowaniem historii ich wystąpienia.
11. AUDYT

Ma umożliwić co najmniej:

1. możliwość bieżącego dostępu do funkcjonalności: planowanie działalności, zarządzanie ryzykiem, monitorowanie i sprawozdawczość, ankiety, zarządzanie zadaniami (w tym niezgodnościami),
2. możliwość generowania raportów i zestawień dotyczących ryzyk wpływających na realizację celów i zadań MAP, w tym ryzyk dotyczących cyberbezpieczeństwa, danych osobowych, korupcyjnych,
3. możliwość generowania raportów i zestawień, w tym o charakterze statystycznym   
   np. dotyczących stopnia realizacji planów,
4. możliwość sporządzania ankiet, publikowania ich w Systemie, generowania statystyk i raportów z wyników,
5. szablon do przeprowadzania analizy ryzyka na potrzeby planu audytu oraz zadań zapewniających,
6. możliwość sporządzania planów audytu: rocznych i strategicznych (wieloletnich tj. max. 5 lat),
7. zapewnienie repozytorium dokumentów związanych z audytem,
8. zapewnienie wersjonowania dokumentacji i możliwość śledzenia zmian.

**Wymagania bezpieczeństwa oraz wymagania techniczne dotyczące systemu**

System powinien działać w chmurze na bezpiecznej infrastrukturze firmy zapewniającej ciągłość świadczenia usługi oraz odpowiedni poziom cyberbezpieczeństwa i ochrony danych osobowych, zgodnie z wymaganymi przepisami.

System zapewni możliwość:

1. logowania aktywności użytkownika wraz z przeglądaniem logów przez uprawnione osoby i możliwością eksportowania logów,
2. nadawanie użytkownikom różnych poziomów uprawnień z uwzględnieniem funkcji, jaką pełnią w MAP,
3. wielostopniowej ścieżki akceptacji dokumentów, zgodnie z przyjętą w MAP hierarchią służbową (co najmniej 4-poziomowa),
4. edytowania/poprawiania wprowadzanych danych przez użytkowników (wersjonowanie dokumentów),
5. zarządzania systemem uprawnień oraz kontami użytkowników, pozwalające na takie działanie jak: podgląd dokumentacji, zarządzanie, koordynowanie, administrowanie dokumentacją,
6. automatycznej wymiany danych pomiędzy funkcjonalnością zarządzanie ryzykiem a pozostałymi funkcjonalnościami,
7. generowanie dokumentów, w tym raportów zbiorczych z celów, zadań oraz mierników przez osoby uprawnione w ogólnodostępnych formatach np. PDF, DOC, DOCX, XLS, XLSX, JPG.

Interfejs Systemu i dokumentacja użytkownika do Systemu będzie w całości w języku polskim. Wykonawca udostępni wersję produkcyjną oraz wersję demo do ćwiczeń.

System powinien być udostępniany Zamawiającemu przez przeglądarkę internetową (interfejs webowy) z interfejsem w całości w języku polskim oraz musi być w pełni kompatybilny z przeglądarkami internetowymi Chrome, Mozilla Firefox oraz Microsoft Edge. Wykonawca zobowiązuje się do zapewnienia wsparcia dla systemu, w co najmniej dwóch najnowszych wersjach każdej z wymienionych przeglądarek, przy czym aktualizacje muszą być wprowadzane niezwłocznie po wydaniu nowych wersji przeglądarek, jednakże nie później niż w terminie 30 dni od ich publikacji.

Wykonawca zobowiązuje się do zapewnienia dostępności systemu 24/7 (godz./dni w tygodniu).

Usługa musi być dostępna tylko z poziomu adresów IP Zamawiającego lub za pośrednictwem VPN (*site to site*).

Wykonawca zobowiązany jest do zgłaszania incydentów bezpieczeństwa oraz dostarczania raportów. Incydent bezpieczeństwa rozumiany jest jako pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub serię takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań Systemu w MAP i zagrażają bezpieczeństwu informacji. Incydent musi być zgłoszony Zamawiającemu w ciągu 1 godziny od jego wykrycia. Pełny raport dotyczący incydentu, wraz z analizą przyczyn i podjętymi działaniami naprawczymi, powinien być dostarczony w ciągu 20 godzin od jego wykrycia.

Wykonawca dostosowuje się do wymagań prawnych, organizacyjnych i technicznych zapewniających cyberbezpieczeństwo w modelach chmur obliczeniowych, zgodnie z dokumentem *Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO)*, na Poziomie SCCO2: *Kontrolowane informacje urzędowe*.

Wykonawca musi spełnić następujące wymagania dotyczące polityki backupu i odtworzenia:

1. kopie zapasowe tworzone są co 24 godziny, z przechowywaniem przez minimum 90 dni,
2. backupy muszą być szyfrowane,
3. usługa przywracania danych musi być dostępna w czasie do 12 godzin od zgłoszenia Zamawiającego.

Wymagania w zakresie logowania muszą być zgodne z regulacjami wewnętrznymi Zamawiającego w zakresie:

1. długości i złożoności hasła,

* długość hasła wynosi co najmniej 12 znaków,
* zawiera małe i wielkie litery, cyfry oraz znaki specjalne (!, @, #, $, &, itp.),

1. częstotliwości jego zmiany,

* zmiany hasła nie rzadziej niż co 45 dni,

1. metod uwierzytelniania.

System musi umożliwiać włączenie i wyłączenie funkcji wielostopniowego uwierzytelniania.

Wykonawca zapewnieni dostęp w technologii z wykorzystaniem bezpiecznego i szyfrowanego protokołu HTTPS.

System powinien mieć możliwość transferów logów do systemu klasy SIEM\SOAR, a także zapewniać separację zasobów Zamawiającego od innych klientów.

1. Dz.U. z 2023 r. poz. 1270. [↑](#footnote-ref-1)
2. Dz.U. Nr 187, poz. 1254. [↑](#footnote-ref-2)
3. Dz.U. z 2023 r. poz. 1440. [↑](#footnote-ref-3)
4. Dz.U. z 2024 r. poz. 307. [↑](#footnote-ref-4)
5. Dz.U. z 2019 r. poz. 1781. [↑](#footnote-ref-5)
6. Dz.U. z 2024 r. poz. 34. [↑](#footnote-ref-6)
7. Dz.U. z 2024 r. poz. 773. [↑](#footnote-ref-7)
8. Dz.Urz.UE.L Nr 119, str. 1. [↑](#footnote-ref-8)
9. Dz.U. z 2018 r. poz. 506. [↑](#footnote-ref-9)
10. Dz. Urz.MRiF z 2016 poz. 28. [↑](#footnote-ref-10)