



Załącznik nr 5. Opis funkcjonalny aplikacji udostępnionej w chmurze obliczeniowej

WYMAGANIA OGÓLNE

1. Aplikacja musi zapewniać wspomaganie elektroniczne procesów: wdrożenia, prowadzenia i aktualizacji dokumentacji SZBI oraz analizy i raportowania ryzyk bezpieczeństwa informacji w jednostkach administracji publicznej zgodnie z: §20 rozp. KRI, normą ISO 27001 oraz ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz dyrektywą NIS2.
2. Aplikacja powinna stanowić kluczowe narzędzie do monitorowania i przeglądania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji.
3. Aplikacja powinna zapewniać automatyzację procesu wdrożenia SZBI w jednostkach podległych JST.
4. Aplikacja powinna zapewniać redukcję kosztów związanych z bieżącym audytowaniem i wdrożeniem SZBI.
5. Aplikacja powinna zapewniać szybką wymianę danych i komunikację w zakresie incydentów bezpieczeństwa przetwarzania danych jednostek.
6. Aplikacja powinna zapewniać wsparcie procesu szkoleniowego i zapoznania z dokumentacją SZBI przez użytkowników aplikacji.
7. Aplikacja musi stanowić repozytorium centralne SZBI w szczególności: procedur obsługi incydentów, ciągłości działania oraz analizy ryzyk w jednostkach sektora publicznego zgodnie z §20 rozporządzenia Rady Ministrów z dnia 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
8. Aplikacja powinna zapewniać szybką weryfikację poprawności i spójności wdrożonej dokumentacji SZBI.
9. Aplikacja powinna zapewniać możliwość przejścia na formę elektroniczną wdrażania SZBI w jednostkach zgodnie z uzgodnionymi szablonami dokumentów na poziomie JST.

OPIS FUNKCJONALNOŚCI APLIKACJI:

1. Praca aplikacji w formie usługi SaaS (usługi w chmurze) z dowolnego urządzenia połączonego z Internetem (bez konieczności instalacji dodatkowych komponentów).
2. Odzworowanie struktury organizacyjnej JST, w szczególności wprowadzenie jednostek i komórek organizacyjnych wraz z kontami dla pracowników oraz przydzielaniem im określonych ról i uprawnień (obsługa do 5000 kont).
3. Indywidualna konfiguracja parametrów dokumentacji SZBI poprzez uzgodnione formularze dla każdej jednostki organizacyjnej.
4. Zarządzanie bezpieczeństwem w oparciu o zdefiniowane modele procesów biznesowych.
5. Kokpit do zarządzania dokumentacją SZBI wraz z automatyczną kontrolą zgodności wdrożonej wersji dokumentu z najnowszym opublikowanym wzorcem.
6. Pełna rozliczalność wszystkich operacji wykonywanych przez użytkownika w aplikacji SZBI zgodnie z RODO i KRI.
7. Obsługa procesu udostępniania aktualnych dokumentów SZBI dla pracowników jednostek i komórek organizacyjnych.
8. Wewnętrzne forum dyskusyjne zapewniające elektroniczne konsultacje dokumentacji SZBI.



Cyberbezpieczny Samorząd

9. Automatyczne raportowanie stanu zapoznania z poszczególnymi elementami dokumentacji SZBI w tym PBI przez uprawnionych pracowników jednostek i komórek organizacyjnych.
10. Podgląd bieżących dokumentów SZBI jednostek przez uprawnionych audytorów wewnętrznych.
11. Generowanie automatycznie redagowanych dokumentów SZBI / PBI do plików PDF.
12. Zachowanie pełnej historii zmian dokumentacji SZBI.
13. Definiowanie w aplikacji procesów biznesowych (diagram oraz opis), które pozwalają na ujednolicenie kluczowych procedur bezpieczeństwa oraz wskazanie użytkownikom zakresu czynności / odpowiedzialności.
14. Automatyczna inicjalizacja mapowania użytkowników aplikacji w procesach biznesowych zależna od określonych w Jednostce ról użytkowników.
15. Zabezpieczenie przed błędnym przypisaniem użytkownika do roli biznesowej (np. Kierownik Jednostki nie może mieć roli Inspektora Ochrony Danych).
16. Zgłaszanie incydentów i zagrożeń przez użytkowników systemu bezpośrednio do koordynatorów ze strony JST.
17. Utworzenie oraz udostępnienie planów reagowania na incydenty dla pracowników.
18. Zapewnienie zarządzania incydentami w podległych jednostkach publicznych JST przez koordynatorów.
19. Definiowanie oraz dokumentowanie działań prowadzonych po wystąpieniu incydu/zagrożenia.
20. Prowadzenia rejestrów naruszeń bezpieczeństwa informacji i ochrony danych osobowych.
21. Prowadzenie wspólnej bazy ryzyk bezpieczeństwa informacji na poziomie JST przez uprawnione osoby odpowiedzialne za cyberbezpieczeństwo.
22. Identyfikacja i ocena ryzyk z odniesieniem do wybranych aktywów i realizowanych celów, zadań i procesów jednostek organizacyjnych zgodnie z zatwierdzoną procedurą.
23. Nadawanie priorytetów na poziomie JST dla zidentyfikowanych ryzyk oraz podejmowanie zdefiniowanych działań obniżających poziomy ryzyk przez uprawnione osoby odpowiedzialne za cyberbezpieczeństwo.
24. Prowadzenie identyfikacji i szacowania ryzyk w oparciu o wspólną bazę ryzyk zgodnie z normą ISO 27005.
25. Generowanie raportów zbiorczych wg wybranych parametrów dla zidentyfikowanych ryzyk bezpieczeństwa informacji w jednostkach JST objętych aplikacją.

