**Obowiązki Wykonawcy z obszaru bezpieczeństwa informacji**

1. W ramach realizacji Przedmiotu umowy Wykonawca zobowiązuje się do:
   1. zapewnienia niezakłóconego dostępu do Systemu, o którym mowa w § 2 Umowy;
   2. bieżącego monitorowania platformy sprzętowo – systemowej, na której zainstalowano System, w szczególności pod kątem wydajności, kompatybilności z oprogramowaniem systemowym serwerów i baz danych oraz prób nieautoryzowanego dostępu do przetwarzanych na nich informacji;
   3. przeciwdziałania próbom włamania, zniszczenia danych oraz nieautoryzowanego dostępu do danych Zamawiającego przetwarzanych z wykorzystaniem Systemu;
   4. podejmowania działań naprawczych w przypadku zagrożenia bezpieczeństwa świadczonych dla Zamawiającego usług, zakłóceń w zakresie ich wydajności oraz wystąpienia błędów baz danych;
   5. administrowania oprogramowaniem systemowym, narzędziowym i aplikacyjnym, w tym tworzenia kopii bezpieczeństwa i ochrony zasobów informacyjnych Zamawiającego przetwarzanych z wykorzystaniem Systemu;
   6. instalacji poprawek, w szczególności dotyczących bezpieczeństwa, oraz aktualizacji oprogramowania niezbędnego do prawidłowej pracy udostępnianej platformy sprzętowo – systemowej, na której zainstalowano System, do wersji aktualnie wspieranych przez producentów systemu operacyjnego i bazy danych; przy czym wymagane jest, aby Wykonawca wykorzystał wspieraną wersję stabilną (produkcyjną) danego komponentu oraz dopasował pozostałe komponenty w ramach udostępnianego środowiska do udostępnianych przez producenta poprawek dla użytkowanej wersji w terminie maksymalnie 12 miesięcy od udostępniania poprawki oraz w terminie maksymalnie 1 tygodnia od udostępnienia aktualizacji bezpieczeństwa;
   7. zapewnienia dostępności Systemu w wymiarze nie mniejszej niż 95% w skali roku, w całym okresie obowiązywania umowy, z wyłączeniem przerw wynikających z okien serwisowych, ustalonych pomiędzy Stronami;

Dostępność Systemu będzie obliczana wg następującego wzoru:



gdzie:

X – oznacza procent dostępności;

gn – oznacza liczbę godzin niedostępności Systemu w danym roku

d – oznacza łączną liczbę dni w danym roku

* 1. zapewnienie dostępu do wiedzy w zakresie korzystania z Systemu zgodnie z § 3 ust. 2 Umowy;
  2. przyjmowania zgłoszeń o awariach i ich obsługi zgodnie z § 8 Umowy;

1. Wykonawca oświadcza, że w zakresie standardów techniczno-organizacyjnych zobowiązuje się zapewnić realizację następujących wymagań tytułem wykonania Przedmiotu Umowy:
2. udostępniana platforma sprzętowo - systemowa, na której zainstalowano System wykorzystywana do przetwarzania danych Zamawiającego, w tym danych osobowych znajduje się na terytorium Rzeczpospolitej Polskiej lub państw członkowskich Europejskiego Obszaru Gospodarczego;
3. dostęp do Systemu odbywa się wyłącznie po połączeniu szyfrowanym https, z zachowaniem następujących standardów:
   * 1. konfiguracja połączenia HTTPS otrzymuje ocenę A+ z testów na stronie https://www.ssllabs.com lub innej ustalonej z Zamawiającym, a wszelkie ewentualne odstępstwa w tym zakresie muszą zostać z nim ustalone;
     2. użyta zostanie domena ustalona z Zamawiającym o nazwie: …………; **[Należy podać nazwę]**
4. szyfrowanie komunikacji przekazywanych danych z wykorzystaniem technik kryptograficznych i długości kluczy uważanych aktualnie za bezpieczne;
5. logowanie zdarzeń na poziomie umożliwiającym dokładną analizę w przypadku kompromitacji Systemu;
6. możliwość integracji z systemami klasy SIEM (ustandaryzowany log systemowy) – wymóg opcjonalny;
7. zarządzanie uprawnieniami użytkowników poprzez odpowiednią strukturę ról;
8. widoczność portów/usług w sieci Internet ograniczona jest do niezbędnego minimum, dostęp do portów i usług, które nie są niezbędne do prawidłowego działania Systemu powinien zostać maksymalnie ograniczony; wykaz portów/usług publicznie dostępnych oraz niezbędnych do prawidłowego korzystania z funkcjonalności Systemu wraz z ich funkcją i wdrożonymi zabezpieczeniami przesyłanych przez nie danych, znajduje się w dokumentacji Systemu przekazanej Zamawiającemu;
9. wszystkie stosowane przez Wykonawcę komponenty, używają wersji oficjalnie wspieranej i rozwijanej przez producenta danego komponentu;
10. System implementuje odpowiednie mechanizmy w zakresie bezpieczeństwa aplikacji, w celu uzyskania odporności na cyber zagrożenia, w tym 10 najczęstszych ataków według statystyk OWASP (Open Web Application Security Project);
11. System posiada możliwość:
12. konfiguracji i wymuszenia stosowania silnego uwierzytelnienia (Multi-Factor Authentication);
13. definiowania polityki haseł (wymuszanie minimalnej długości, jakości, częstotliwości zmian);
14. rozdzielenie danych produkcyjnych od danych stanowiących kopie zapasowe w taki sposób, aby zabezpieczyć je przed utratą i zapewnić możliwość ich odtworzenia;
15. udostępniana platforma sprzętowo – systemowa, na której zainstalowano udostępniane rozwiązania oraz System poddawane są cyklicznym testom penetracyjnym, nie rzadziej niż raz na rok, pod kątem zagrożeń występujących w sieci Internet celem minimalizacji ryzyka naruszenia poufności, dostępności i integralności danych; wyniki ww. testów będą przekazywane Zamawiającemu do końca danego roku korzystania z jego usług;
16. tworzone przez Wykonawcę kopie zapasowe Systemu są przygotowywane i udostępniane wg schematu:
17. wykonywanie codziennie przyrostowej kopii danych z okresem przechowywania w postaci zaszyfrowanej na bezpiecznym serwerze co najmniej 30 dni;
18. wykonywanie raz w miesiącu całościowej kopii danych z okresem przechowywania w postaci zaszyfrowanej na bezpiecznym serwerze co najmniej 12 miesięcy;
19. okresowe (przynajmniej raz na kwartał) sprawdzanie kopii pod kątem przydatności do odtworzenia danych przechowywanych na kopiach zapasowych;
20. udostępnianie Zamawiającemu wskazanej kopii zapasowej danych w terminie 3 dni roboczych od pisemnego zgłoszenia żądania lub w inny ustalony między Stronami sposób;
21. System jest zgodny ze wszystkimi wytycznymi WCAG 2.1 zawartymi w załączniku do Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.
22. Strony ustaliły, że:
23. Wykonawca zobowiązany jest do przekazywania informacji na temat okoliczności wystąpienia danego incydentu[[1]](#footnote-2) z udziałem danych Zamawiającego, w tym szczegółów technicznych, a jeśli nie jest to możliwe do ustalenia bezpośrednio przez Wykonawcę, pokrywa on koszty usługi zewnętrznej celem ustalenia zakresu, przebiegu i skutków zaistniałego incydentu;
24. w przypadku utraty danych spowodowanych rażącym naruszeniem przez Wykonawcę standardów w obszarze bezpieczeństwa informacji, Wykonawca zobowiązany jest do odtworzenia stanu Systemu sprzed zdarzenia/incydentu, w tym danych Zamawiającego;
25. Zamawiający jest uprawniony do przeprowadzenia skanowania podatności oferowanych rozwiązań za pomocą oprogramowania typu Nessus lub OpenVAS oraz do przeprowadzenia testów penetracyjnych w uzgodnieniu z Wykonawcą.

1. Incydent - naruszenie poufności, dostępności lub integralności danych Zamawiającego. [↑](#footnote-ref-2)