Wymagania związane z przetwarzaniem danych osobowych w Systemie Finansowo-Księgowym do obsługi jednostek edukacyjnych.

1. Dostęp do zasobu możliwy po podaniu dodatkowego loginu i hasła (nie SSO);
2. Usługi i serwisy aplikacji wymagają autoryzacji;
3. Uprawnienia użytkowników aplikacji różnicowane co najmniej na poziomach do odczytu/zapisu/kasowania;
4. Platforma posiada role lub grupy z możliwością przyznawania uprawnień skutkujące ograniczeniem dostępu do danych oraz funkcjonalności zgodnie z zasadą wiedzy koniecznej, oznacza to między innymi nadawanie uprawnień do podzbioru danych zarówno w zakresie wybranych wierszy jak również kolumn tabel danych;
5. Unikalny identyfikator użytkownika może być przydzielony tylko jednemu użytkownikowi;
6. Platforma wylogowuje użytkownika automatycznie po zdefiniowanym czasie bezczynności;
7. Platforma ostrzega przed kolejnym (drugim i kolejnym) zalogowaniem się tego samego użytkownika w tym samym czasie (do systemu/aplikacji, nie do domeny);
8. Po określonej liczbie nieudanych prób logowania Platforma blokuje konto użytkownika (Administrator ma możliwość odblokowania konta);
9. Platforma posiada funkcjonalność dotyczącą wymuszenia zmiany hasła przy najbliższym logowaniu (jeśli logowanie inne niż na użytkownika domenowego, w przeciwnym razie implementuje ustawienia domeny);
10. Platforma posiada funkcjonalność dotyczącą wymuszenia zmiany hasła co określony interwał czasowy konfigurowalny przez Administratora;
11. Platforma implementuje elementarne wymagania dotyczące co najmniej ‘mocy’ hasła użytkownika i niepowtarzalności n ostatnich haseł;
12. Kontrolka służąca do podania loginu nie podpowiada i nie pamięta poprzednio wprowadzanych wartości;
13. Działania użytkownika w systemie są mu przypisywane na podstawie unikalnego identyfikatora (domenowego lub loginu do aplikacji);
14. Log systemowy zawiera informację o każdym uruchomieniu aplikacji przez użytkownika;
15. Log systemowy zawiera informację o każdym zakończeniu pracy-wylogowaniu się z aplikacji przez użytkownika;
16. Log systemowy lub rekord danych zawiera informację o czasie jego utworzenia (dodanie nowego rekordu);
17. Log systemowy lub rekord danych zawiera identyfikator użytkownika, który utworzył nowy rekord;
18. Log systemowy lub rekord danych zawiera informację o czasie ostatniego zapisania rekordu;
19. Log systemowy lub rekord danych zawiera identyfikator użytkownika, który ostatni zapisał rekord;
20. Log systemowy lub rekord danych zawiera pełną historię o czasach i użytkownikach zapisujących rekord (tylko data, czas i identyfikator);
21. Platforma posiada mechanizm eksportu logów systemowych na wskazany zasób lub zapisuje

je we własnym syslogu z zapewnieniem dostępu dla systemu SIEM (odczyt); wykonawca otrzyma informację o strukturze rekordu logu;

22. Platforma musi być opracowana z domyślnymi ustawieniami, które chronią prawa osób, których dane dotyczą i zabezpieczają prywatność;
23. Wymagany protokół HTTPS z odpowiedniej klasy certyfikatem;
24. Platforma ostrzega o nieaktualnej wersji przeglądarki (informacje o wersji może aktualizować administrator w parametrach konfiguracyjnych);
25. Po zakończeniu umowy musi być przekazana kopia danych, w tym również logów systemowych zawierających pełne informacje o dostępie do danych w czasie trwania umowy oraz „archiwum wewnętrznego" zawierającego dane, które już nie są przetwarzane w terminie do 30 dni;
26. Wykonawca po swojej stronie zapewni podstawowe środki zabezpieczające Platformę przed niepowołanym dostępem, w tym:

    Dla sieci publicznej/Internetu

    - system wykrywania ataków hackerskich IDS/IPS
    - dostęp VPN (szyfrowany dostęp zdalny)

    Dla sieci prywatnej/wewnętrznej

    - dostęp VPN (szyfrowany dostęp zdalny)
    - system kontroli dostępu do sieci wewn. (802.1x)
    - zabezpieczony system przydziału adresów IP
    - zabezpieczone punkty dystrybucyjne sieci (kontrola dostępu, redundancja, zasilanie, klimatyzacja)
    - system monitoringu i raportowania stanu i zarządzania infrastrukturą
    - system ochrony antywirusowej
27. Wykonawca po swojej stronie zapewni dodatkowe środki zabezpieczające Platformę przed niepowołanym dostępem, w tym:

    Dla sieci publicznej/Internetu

    - firewall – zintegrowany system
    - dostęp do Internetu chroniony przed atakami hackerskimi (DDos)
28. Wykonawca po swojej stronie odpowiednio zabezpieczy centrum przetwarzania danych, minimalne wymagania:

    - system sygnalizacji włamania i napadu
    - system monitoringu wizyjnego
    - system klimatyzacji precyzyjnej
    - system sygnalizacji pożaru oraz stałych urządzeń gaśniczych
29. Wykonawca po swojej stronie dodatkowo zabezpieczy centrum przetwarzania danych poprzez:

    - system kontroli dostępu
    - system awaryjnego podtrzymania zasilania