Wymagania bezpieczeństwa

W liście wymagań związanych z zapewnieniem bezpieczeństwa Systemu zastosowano następujące zasady dla priorytetów:

Wysoki	Bezwzględnie wymagane.
Średni	Nie wymagane, ale dodatkowo punktowane.
Niski	Nie wymagane, ale dodatkowo punktowane.

ID wymagania	**B1**	
Nazwa	**Bezpieczeństwo danych przechowywanych w systemie**	
Zgłaszający wymaganie	**CUI**	
Nr wymagania	**Opis wymagania**	**Priorytet** (wysoki / średni / niski)
B1.1	Zasób informacyjny dostępny co najmniej po logowaniu domenowym.	wysoki
B1.2	Dostęp do zasobu po podaniu dodatkowego loginu i hasła (nie SSO).	średni
B1.3	Uwierzytelnienie użytkowników w systemie jest dwuskładnikowe.	średni
B1.4	Dostęp do zasobu przyznawany na zasadzie listy dostępu (ACL) - dotyczy np. dyskowych zasobów sieciowych (M: , SFTP:).	wysoki
B1.5	Usługi i serwisy aplikacji wymagają autoryzacji	wysoki
B1.6	Uprawnienia użytkowników aplikacji różnicowane co najmniej na poziomach do odczytu/zapisu/kasowania.	wysoki
B1.7	System posiada role lub grupy z możliwością przyznawania uprawnień skutkujące ograniczeniem dostępu do danych oraz funkcjonalności zgodnie z zasadą wiedzy koniecznej. Oznacza to	wysoki

Fundusze Europejskie Program Regionalny | Rzeczpospolita Polska | DOLNY ŚLĄSK | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

„System transformacji cyfrowej i procesowej w Departamencie Strategii i Rozwoju Miasta Urzędu Miejskiego Wrocławia" nr RPDS.02.01.02-02-0013/21

	między innymi nadawanie uprawnień do podzbioru danych zarówno w zakresie wybranych wierszy jak również kolumn tabel danych.	
B1.8	System umożliwia wyłączenie możliwości wprowadzania danych nadmiarowych, których przetwarzanie nie jest uzasadnione z punktu widzenia celu przetwarzania (minimalizacja danych).	średni
B1.9	Aplikacje nie są dostępne spoza sieci wewnętrznej LAN UMW/CUI.	średni
B1.10	Systemy posiadają dodatkowe zabezpieczenia autoryzujące dostęp (poza loginem i hasłem), np. dostęp tylko dla określonych adresów IP.	średni
B1.11	Unikalny identyfikator użytkownika może być przydzielony tylko jednemu użytkownikowi.	wysoki
B1.12.	Po zdefiniowanym czasie bezczynności następuje automatyczne wylogowanie użytkownika z Systemu.	wysoki
B1.13	System ostrzega przed kolejnym (drugim i kolejnym) zalogowaniem się tego samego użytkownika w tym samym czasie (do systemu/aplikacji, nie do domeny).	wysoki
B1.14	Po kolejnym zalogowaniu się tego samego użytkownika w tym samym czasie (do systemu/aplikacji, nie do domeny) system blokuje dostęp.	średni
B1.15	Po określonej liczbie nieudanych prób logowania system blokuje konto użytkownika (administrator ma możliwość odblokowania konta).	wysoki
B1.16	System przechowuje historię dotyczącą blokowania i odblokowywania kont użytkowników.	średni
B1.17	System posiada funkcjonalność dotyczącą wymuszenia zmiany hasła przy	wysoki

	najbliższym logowaniu (jeśli logowanie inne niż na użytkownika domenowego, w przeciwnym razie implementuje ustawienia domeny).	
B1.18	System posiada funkcjonalność dotyczącą wymuszenia zmiany hasła co określony interwał czasowy – konfigurowalny przez administratora jeśli logowanie inne niż na użytkownika domenowego, w przeciwnym razie implementuje ustawienia domeny).	wysoki
B1.19	System implementuje elementarne wymagania dotyczące co najmniej 'mocy' hasła użytkownika i niepowtarzalności n ostatnich haseł (jeśli logowanie inne niż na użytkownika domenowego, w przeciwnym razie implementuje ustawienia domeny).	wysoki
B1.20	Kontrolka służąca do podania loginu nie podpowiada i nie pamięta poprzednio wprowadzanych wartości.	wysoki
B1.21	Wprowadzanie loginu i hasła przez użytkownika odbywa się na dwóch różnych ekranach/stronach/oknach dialogowych.	średni
B1.22	System informuje o stanie klawisza CapsLock, NumLock oraz typie ustawionej klawiatury.	średni
B1.23	Działania użytkownika w systemie są mu przypisywane na podstawie unikalnego identyfikatora (domenowego lub loginu do aplikacji).	wysoki
B1.24	Log systemowy zawiera informację o każdym uruchomieniu aplikacji przez użytkownika.	wysoki
B1.25	Log systemowy zawiera informację o każdym zakończeniu pracy - wylogowaniu się z aplikacji przez użytkownika.	wysoki

B1.26	Log systemowy zawiera informację o każdym przerwaniu pracy - wylogowaniu użytkownika z powodu bezczynności.	wysoki
B1.27	Log systemowy lub rekord danych zawiera informację o czasie jego utworzenia (dodanie nowego rekordu).	wysoki
B1.28	Log systemowy lub rekord danych zawiera identyfikator użytkownika, który utworzył nowy rekord.	wysoki
B1.29	Log systemowy lub rekord danych zawiera informację o czasie ostatniego zapisania rekordu.	wysoki
B1.30	Log systemowy lub rekord danych zawiera identyfikator użytkownika, który ostatni zapisał rekord.	wysoki
B1.31	Log systemowy lub rekord danych zawiera pełną historię o czasach i użytkownikach zapisujących rekord (tylko data, czas i identyfikator).	wysoki
B1.32	Log systemowy lub rekord danych zawiera pełną informację o dokonywanych zmianach w rekordzie (kto, kiedy i jakie wartości zmienił; zakres logowanych zmian nie musi obejmować wszystkich atrybutów, a tylko newralgiczne).	średni
B1.33	Log systemowy zawiera podstawowe informacje (data, czas, identyfikator, operacja) o wykonywanych operacjach przetwarzania -przeglądanie, edytowanie, tworzenie, kasowanie, indywidualne wydruki, eksportowanie danych, itp.	średni
B1.34	Log systemowy zawiera szczegółowe informacje (data, czas, identyfikator, operacja, zakres, [uzasadnienie]) o wykonywanych operacjach przetwarzania - przeglądanie, edytowanie, tworzenie, kasowanie, indywidualne wydruki, eksportowanie danych, itp.	średni

B1.35	System 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.	wysoki
B1.36	W przypadku gdy różne zakresy danych przetwarzane są w oparciu o różne przesłanki legalizujące (podstawy prawne) system jest tego świadomy i potrafi przypisać konkretne działania/żądania/konsekwencje zrealizowanych żądań do konkretnego zakresu danych wg przesłanki legalizującej.	wysoki
B1.37	W przypadku gdy różne zakresy danych przetwarzane są w oparciu o różne źródła ich pozyskania (od osoby / z innych źródeł) system jest tego świadomy i potrafi przypisać konkretne działania/żądania/konsekwencje zrealizowanych żądań do konkretnego zakresu danych wg źródła pochodzenia.	wysoki
B1.38	W przypadku przetwarzania w systemie danych osobowych (dane osobowe szczególne) system zbiera informację o fakcie wyrażenia przez osobę zgody na przetwarzanie danych osobowych szczególnych.	wysoki
B1.39	System musi być opracowany z domyślnymi ustawieniami, które chronią prawa osób, których dane dotyczą i zabezpieczają prywatność.	wysoki
B1.40	System pozwala na zapisywanie informacji o okresie przechowywania danych i pozwala na raportowanie danych których okres przechowywania wygasa.	wysoki

ID wymagania	**B2**	
Nazwa	**Realizacja w Systemie prawa do: wycofania zgody, usunięcia danych, sprzeciwu, sprostowania, ograniczenia dostępu do danych, informacji o przetwarzaniu, kopii danych, przenoszenia danych**	
Zgłaszający wymaganie	**CUI**	
Nr wymagania	**Opis wymagania**	**Priorytet** (wysoki / średni / niski)
B2.1	System umożliwia drukowanie klauzuli informacyjnej w przypadku zbierania danych bezpośrednio od podmiotu lub źródła danych.	wysoki
B2.2	System przechowuje historię implementowanych w nim żądań osób (kogo dotyczyło, w jakim okresie występowało, jakiego typu żądanie) - chyba że istnieje inny centralny system o takiej funkcjonalności dla wielu systemów/aplikacji.	wysoki
B2.3	Jeżeli system przetwarza dane osobowe w różnych celach to jest tego świadomy i implementuje lub umożliwia oznaczanie danych w oparciu o konkretne cele przetwarzania; takie oznaczenie ma swoje logiczne konsekwencje dla możliwych czynności przetwarzania oraz realizacji praw osób.	wysoki
B2.4	System umożliwia wyszukanie osoby wg określonego zestawu atrybutów, w szczególności wg unikalnych identyfikatorów jeśli występują w systemie, prezentacja wyników wyszukiwania odbywa się „po jednym rekordzie” albo tylko w przypadku znalezienia jednego rekordu w wyniku	wysoki

	zastosowania kryteriów wyszukiwania	
B2.5	system umożliwia wykonanie kompletnego wydruku lub serii wydruków zawierających komplet danych osobowych wskazanej/wyszukanej osoby w przejrzystej jasnej postaci (raport danych osobowych).	wysoki
B2.6	System umożliwia wykonanie kompletnego wydruku lub serii wydruków zawierających komplet danych osobowych wskazanej/wyszukanej osoby w przejrzystej jasnej postaci wraz z metadanymi dotyczącymi operacji wykonywanych na wydrukowanych danych.	wysoki
B2.7	System umożliwia (w wyniku wywołania wbudowanej w niego funkcjonalności) eksportowanie danych dotyczących konkretnej osoby w jednym z następujących formatów danych: txt, csv, xml, json ; dopuszczalne jest wielokrotne wywoływanie funkcjonalności w celu otrzymania kompletu danych, oczekiwane jest jednokrotne wywołanie skutkujące kompletem danych.	wysoki

ID wymagania	**B3**	
Nazwa	**Anonimizacja, pseudonimizacja, szyfrowanie i archiwizowanie danych**	
Zgłaszający wymaganie	**CUI**	
Nr wymagania	**Opis wymagania**	**Priorytet** (wysoki / średni / niski)

B3.1	System posiada wbudowane funkcjonalności umożliwiające wybiórczą lub kompletną anonimizację danych albo wybiórcze lub kompletne usunięcie danych, które nie powinny być już przetwarzane.	wysoki
B3.2	System posiada wbudowane funkcjonalności umożliwiające wybiórczą lub kompletną pseudonimizację danych wraz z możliwością uprawnionego odwrócenia.	wysoki
B3.3	System posiada „archiwum wewnętrzne" do którego dane mogą być przenoszone (ręcznie lub automatycznie) po zadanym okresie przetwarzania lub po spełnieniu innych warunków.	wysoki
B3.4	Wszystkie dane przechowywane w zasobie informacyjnym IT (baza danych, pliki, ...) są szyfrowane z wykorzystaniem algorytmów, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.	średni

ID wymagania	**B4**	
Nazwa	**Profilowanie danych i/lub automatyczne podejmowanie decyzji**	
Zgłaszający wymaganie	**CUI**	
Nr wymagania	**Opis wymagania**	**Priorytet** (wysoki / średni / niski)
B4.1	Wykonawca dostarczy dokładny opis algorytmu na podstawie którego odbywa się profilowanie i/lub następuje automatyczne podejmowanie decyzji w systemie.	wysoki

B4.2	System przechowuje informacje o przekazaniu danych innym podmiotom, np. w postaci flag .	średni

ID wymagania	**B5**	
Nazwa	**Aplikacje WWW gdzie interfejsem jest przeglądarka internetowa**	
Zgłaszający wymaganie	**CUI**	
Nr wymagania	**Opis wymagania**	**Priorytet** (wysoki / średni / niski)
B5.1	Wymagany protokół HTTPS z odpowiedniej klasy certyfikatem.	wysoki
B5.2	Aplikacja ostrzega o nieaktualnej wersji przeglądarki (informacje o wersji może aktualizować administrator w parametrach konfiguracyjnych).	wysoki
B5.3	Aplikacja uniemożliwia pracę w przypadku zbyt starej wersji przeglądarki (informacje o wersji może aktualizować administrator w parametrach konfiguracyjnych).	wysoki
B5.4	Aplikacja spełnia wymagania Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych z uwzględnieniem wymagań określonych w pkt 9, 10 i 11 normy EN 301 549 V2.1.2, w szczególności w zakresie: • funkcjonalności, • kompatybilności, • nawigacji, • postrzegalności, • zrozumiałości, • deklaracji dostępności, • obsługi żądania zapewnienia	wysoki

	dostępności cyfrowej.	
B5.5	Na stronie WWW jest opublikowana deklaracja dostępności (art. 10 ustawy o dostępności cyfrowej) zgodnie dokumentem https://mc.bip.gov.pl/objasnienia-prawne/warunki-techniczne-publikacji-oraz-struktura-dokumentu-elektronicznego-deklaracji-dostepnosci.html (lub jego kolejnymi wersjami) określającym warunki techniczne publikacji Deklaracji Dostępności oraz strukturę dokumentu elektronicznego Deklaracji Dostępności.	wysoki

ID wymagania	**B6**	
Nazwa	**Dane osobowe przetwarzane na podstawie zgody oraz prezentowanie klauzul informacyjnych**	
Zgłaszający wymaganie	**CUI**	
Nr wymagania	**Opis wymagania**	**Priorytet** (wysoki / średni / niski)
B6.1	System umożliwia obsługę udzielania i wycofywania zgody w ten sam łatwy i jednoznaczny sposób.	wysoki
B6.2	System przechowuje i prezentuje użytkownikowi historię udzielanych i wycofywanych zgód (operacja, data i czas).	wysoki
B6.3	System wersjonuje treści klauzul zgody.	wysoki
B6.4	System posiada opisaną i zaakceptowaną przez IOD wewnętrzną logikę obsługującą zmiany treści zgód.	wysoki

B6.5	System prezentuje klauzulę informacyjną gdy dane o osobie wprowadza ona sama/opiekun prawny.	wysoki
B6.6	System wersjonuje klauzule informacyjne.	wysoki
B6.7	System posiada opisaną i zaakceptowaną przez IOD wewnętrzną logikę obsługującą zmiany treści klauzul informacyjnych.	wysoki
B6.8	Jeśli klauzule informacyjne są prezentowane w oparciu o zaakceptowana logikę, to system przechowuje i prezentuje użytkownikowi historię przyjętych do wiadomości treści klauzul informacyjnych.	wysoki
B6.9	System zapewnia, że żadne pozycje wymaganych zgód nie są domyślnie ustawione w pozycji akceptacji – wymagana jest świadoma akcja użytkownika w celu udzielenia i wycofania zgody.	wysoki
B6.10	System zapewnia, że domyślne ustawienia konfiguracyjne i parametryczne (o ile istnieją) realizują maksymalny możliwy poziom ochrony prywatności podmiotu danych; dla zmiany zasad ochrony prywatności wymagana jest świadoma akcja użytkownika.	wysoki

ID wymagania	**B7**	
Nazwa	**Aplikacje w modelu SaaS**	
Zgłaszający wymaganie	**CUI**	
Nr wymagania	**Opis wymagania**	**Priorytet** (wysoki / średni / niski)

B7.1	Po zakończeniu umowy wymagane jest przekazanie kopii 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.	wysoki
B7.2	Administrator systemu (pracownik CUI) będzie miał zapewniony dostęp do nadawania uprawnień w systemie, wymuszania zmiany hasła, dostęp do logów systemowych	wysoki
B7.3	Wykonawca po swojej stronie zapewni środki zabezpieczające system 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	wysoki
B7.4	Wykonawca po swojej stronie zapewni dodatkowe środki zabezpieczające system przed niepowołanym dostępem, w tym: Dla sieci publicznej/Internetu – firewall – zintegrowany system	wysoki

	– dostęp do Internetu chroniony przed atakami hackerskimi (DDos)	
B7.5	Wykonawca po swojej stronie zapewni dodatkowe środki zabezpieczające system przed niepowołanym dostępem, w tym: Dla sieci publicznej/Internetu – system kontroli treści – system bezpieczeństwa usługi DNS (firewall DNS)	średni
B7.6	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	wysoki
B7.7	Wykonawca po swojej stronie dodatkowo zabezpieczy centrum przetwarzania danych poprzez: – system kontroli dostępu – system awaryjnego podtrzymania zasilania	wysoki