

Tabela zgodności z wymaganiami bezpieczeństwa - Skróty i Definicje

Lp.	Opis
Definicja 1	<b>ADFS</b> - Active Directory Federation Services (ang.) – usługa bezpiecznego udostępniania tożsamości cyfrowej z zaufanymi partnerami
Definicja 2	<b>API</b> - Application Programming Interface (ang.) – interfejs programistyczny aplikacji pozwalający na komunikację z aplikacją
Definicja 3	<b>CRL</b> - Certificate Revocation List (ang.) - lista unieważnionych certyfikatów
Definicja 4	<b>CPD</b> - Centrum Przetwarzania Danych (ang. Data center) – infrastruktura budowlana i środowiskowa zapewniająca wymagane poziomy dostępności i ciągłość usług
Definicja 5	<b>CSP</b> - Cloud Service Provider (ang.) – dostawca usług w chmurze
Definicja 6	<b>DMZ</b> - Demilitarized zone (ang.) – strefa zdemilitaryzowana lub ograniczonego zaufania
Definicja 7	<b>HTTP</b> - Hypertext Transfer Protocol (ang.) – protokół w warstwie aplikacyjnej służący do wymiany informacji pomiędzy rozproszonymi systemami informacyjnymi, używany do obsługi stron WWW
Definicja 8	<b>HSTS</b> - HTTP Strict Transport Security (ang.) - mechanizm zabezpieczenia serwowanych stron polegający na blokowaniu zmian w parametrach protokołu
Definicja 9	<b>HTML</b> - HyperText Markup Language (ang.) – język znaczników wykorzystywany do tworzenia stron WWW
Definicja 10	<b>HTTPS</b> - Hypertext Transfer Protocol Secure (ang.) – zabezpieczony HTTP poprzez zastosowanie SSL/TLS
Definicja 11	<b>IAM</b> - Identity and Access Management (ang.) – zarządzanie tożsamością i dostępem
Definicja 12	<b>MBCO</b> - Minimum Business Continuity Objective - minimalny poziom odtworzenia usługi teleinformatycznej, który jest akceptowalny dla Spółki do osiągnięcia jej celów biznesowych w sytuacji krytycznej
Definicja 13	<b>MFA</b> - Multi Factor Authentication (ang.) - Uwierzytelnianie wieloskładnikowe, metoda uwierzytelniania, która wymaga od użytkownika podania co najmniej dwóch niezależnych czynników (np. <b>2FA</b> z hasłem jednorazowym) w celu potwierdzenia tożsamości. Te czynniki mogą obejmować coś, co użytkownik wie (np. hasło), coś, co posiada (np. telefon), oraz coś, co jest unikalne dla użytkownika (np. odcisk palca, PIN, token sprzętowy lub programowy)
Definicja 14	<b>PGE, PGE S.A.</b> - PGE Polska Grupa Energetyczna S.A.
Definicja 15	<b>PIM</b> - Privileged Identity Management (ang.) – zarządzanie dostępem do Kont Technicznych
Definicja 16	<b>OWASP</b> - Open Web Application Security Project (ang.) – międzynarodowa organizacja, której celem są działania na rzecz poprawy bezpieczeństwa oprogramowania
Definicja 17	<b>OWASP TOP 10</b> - dziesięć najczęstszych podatności i błędów występujących w wytwarzanym oprogramowaniu według organizacji OWASP
Definicja 18	<b>RCB</b> - Rządowe Centrum Bezpieczeństwa, opracowania i zalecenia w kontekście Narodowego Programu Ochrony Infrastruktury Krytycznej
Definicja 19	<b>RODO</b> - Ogólne rozporządzenie o ochronie danych, inaczej rozporządzenie o ochronie danych osobowych, GDPR (ang. General Data Protection Regulation.) – rozporządzenie unijne, zawierające przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych.
Definicja 20	<b>RPO</b> - Recovery Point Objective - poziom akceptowalnej utraty danych; maksymalny okres pomiędzy czasem wykonania ostatniej kopii zapasowej danych, a momentem wystąpienia zakłócenia lub awarii, skutkującego utratą tych danych; np. RPO = 24h oznacza akceptację utraty danych z całego dnia
Definicja 21	<b>RTO</b> - Recovery Time Objective - czas krytyczny/czas odtworzenia – docelowy czas przywrócenia realizacji usługi teleinformatycznej na uzgodnionym wcześniej minimalnym poziomie (MBCO), np. RTO = 4h oznacza konieczność odtworzenia usługi na poziomie MBCO maksymalnie w ciągu 4 godzin od wystąpienia przerwy
Definicja 22	<b>SaaS</b> - Software as a Service (ang.) – oprogramowanie świadczone jako usługa w chmurze obliczeniowej
Definicja 23	<b>SIEM</b> - Security Information and Event Management (ang.) – bezpieczeństwo informacji i zarządzanie zdarzeniami
Definicja 24	<b>SLA</b> - Service Level Agreement (ang.) – umowa o gwarantowanym poziomie świadczenia usług
Definicja 25	<b>SSL</b> - Secure Socket Layer (ang.) – protokół w warstwie transportowej/sesyjnej zapewniający poufność, integralność oraz uwierzytelnienie serwera
Definicja 26	<b>SSO</b> - Single Sign-on (ang.) - możliwość jednorazowego zalogowania się do usługi sieciowej i uzyskania dostępu do wszystkich autoryzowanych zasobów zgodnych z tą usługą
Definicja 27	<b>Spółka, Spółki</b> - podmiot / podmioty prawa handlowego wchodzące w skład Grupy Kapitałowej PGE
Definicja 28	<b>TLS</b> - Transport Layer Security (ang.) - protokół w warstwie transportowej/sesyjnej zapewniający poufność, integralność oraz uwierzytelnienie serwera
Definicja 29	<b>uKSC</b> - ustawa o Krajowym Systemie Cyberbezpieczeństwa
Definicja 30	<b>URI</b> - Uniform Resource Identifier (ang.) – ujednolicony identyfikator jednoznacznie wskazujący na zasób
Definicja 31	<b>XSS</b> - Cross Site Scripting – możliwości osadzenia kodu w treści atakowanej strony
Definicja 32	<b>Administrator Systemu Teleinformatycznego (Administrator)</b> - osoba posiadająca odpowiedni poziom uprawnień i odpowiedzialności za System Teleinformatyczny lub element infrastruktury teleinformatycznej. Osoba ta zarządza i sprawuje nadzór nad Systemem Teleinformatycznym lub innym elementem infrastruktury teleinformatycznej od strony technicznej.
Definicja 33	<b>Bezpieczeństwo Informacji</b> -zapewnienie Poufności, Integralności i Dostępności przetwarzanych informacji czyli zabezpieczanie jej przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem.
Definicja 34	<b>Dostępność</b> - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.
Definicja 35	<b>Dziennik Systemu Teleinformatycznego / Dziennik</b> – opis działań Administratora, które wynikają z bezpiecznej eksploatacji Systemu (co najmniej: zakładanie i blokowanie Kont, nadawanie, modyfikacja i usuwanie uprawnień, czynności konserwacyjne, wykonywanie kopii zapasowych), lub z incydentów Bezpieczeństwa Informacji.
Definicja 36	<b>Grupa Kapitałowa PGE (GK lub GK PGE)</b> – PGE oraz Spółki względem których PGE posiada status spółki dominującej w rozumieniu artykułu 4 § 1 punkt 4 kodeksu spółek handlowych.
Definicja 37	<b>Hasło</b> - ciąg znaków, który służy do uwierzytelniania w Systemie Teleinformatycznym.
Definicja 38	<b>HTTP cookie, Cookie</b> – wysłany przez aplikację webową i przechowywany przez przeglądarkę ciąg znaków, wykorzystywany – przesyłany - w dalszej części komunikacji z przeglądarki do aplikacji webowej.
Definicja 39	<b>Identyfikator w Systemie Teleinformatycznym (Identyfikator)</b> - unikalny ciąg znaków jednoznacznie identyfikujący w Systemie Teleinformatycznym Użytkownika lub inny System Teleinformatyczny.
Definicja 40	<b>Integralność</b> - właściwość zapewnienia dokładności i kompletności. Integralność informacji/danych - oznacza, że dane nie będą w nieautoryzowany lub przypadkowy sposób zmodyfikowane przez nieuprawnione osoby.
Definicja 41	<b>Konto</b> - zbiór praw dostępu do Systemu Teleinformatycznego, dedykowany dla Użytkownika lub innego Systemu Teleinformatycznego identyfikowanych przez Identyfikator i Środki Uwierzytelniania
Definicja 42	<b>Konto Techniczne</b> – Konto z którego korzysta więcej niż jeden Użytkownik i/lub System, nie przynależące do określonego Użytkownika.
Definicja 43	<b>Konto Techniczne Interaktywne</b> – Konto Techniczne, którego uprawnienia umożliwiają wykonywanie określonych czynności administracyjnych w Systemie z możliwością zalogowania się na to Konto (lokalnie lub zdalnie), uzyskania dostępu do konsoli systemowej i wykonywania poleceń administracyjnych.
Definicja 44	<b>Konto Techniczne Nieinteraktywne</b> – Konto Techniczne, którego uprawnienia umożliwiają wykonywanie określonych czynności administracyjnych w Systemie bez możliwości uzyskania dostępu do konsoli systemowej po zalogowaniu się na to Konto.
Definicja 45	<b>Konto Serwisowe</b> – Konto Techniczne, którego uprawnienia umożliwiają wykonywanie określonych czynności w Systemie i używane do cyklicznych czynności serwisowych (np. usługi serwisowe, kopia zapasowa).
Definicja 46	<b>Konto Współdzielone</b> – Konto Techniczne Interaktywne nie będące Kontem Serwisowym wykorzystywane między innymi w celach technicznej obsługi Systemu Teleinformatycznego.
Definicja 47	<b>Plan Ciągłości Działania</b> – zbiór Planów Awaryjnych, procedur odtworzenia usług na wypadek awarii, Instrukcji technicznych, Scenariuszy Awarii oraz mapy powiązań pomiędzy nimi opracowany dla Systemu, zapewniający dotrzymanie uzgodnionych parametrów usługi.
Definicja 48	<b>Poufność</b> - właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
Definicja 49	<b>Przetwarzanie Informacji</b> - jakiegokolwiek operacje wykonywane na informacji, w szczególności takie jak ich zbieranie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie, przesyłanie i usuwanie.
Definicja 50	<b>Ransomware</b> – oprogramowanie, które blokuje dostęp do Systemu lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego
Definicja 51	<b>Strefa zdemilitaryzowana (DMZ)</b> - jest to wydzielany na zaporce sieciowej (ang. firewall) obszar sieci komputerowej nienależący ani do sieci wewnętrznej (tj. tej chronionej przez zaporę), ani do sieci zewnętrznej (tej przed zaporą; na ogół jest to Internet).
Definicja 52	<b>System Teleinformatyczny (System)</b> - zespół środków technicznych wraz z oprogramowaniem tworzący logiczną i nierzeczwalną całość wyodrębnioną ze względu na dostarczaną funkcjonalność przy założeniu, że głównym jego celem jest Przetwarzanie Informacji.
Definicja 53	<b>Środki Uwierzytelniania</b> - hasła, hasła jednorazowe, klucze i certyfikaty cyfrowe, tokeny sprzętowe (karty, klucze, transpondery), sygnatury biometryczne lub ich kombinacje umożliwiające skuteczne uwierzytelnienie Użytkownika w Systemie.
Definicja 54	<b>Użytkownik</b> - osoba uprawniona do korzystania z Systemu Teleinformatycznego.



Tabela zgodności z wymaganiami bezpieczeństwa

Grupa wymagań	Opis warunku
<b>POSTANOWIENIA OGÓLNE</b>	
Postanowienia Ogólne	Następujące słowa kluczowe są używane w dokumencie do określenia zawartego wymagania: a. słowa MUSI, WYMAGANY lub NIE MOŻE, ZABRANIONE oznaczają, że treść zapisu musi być bezwzględnie przestrzegana, b. słowa POWINNO, ZALECANE lub NIE POWINNO, NIEZALECANE, MOŻE oznaczają, że dopuszczalne jest niezastosowanie się do treści zapisu. Muszą ku temu zaistnieć szczególne okoliczności lub uzasadnione powody <u>zatwierdzone przez Zamawiającego</u>
Postanowienia Ogólne	ZALECANE jest unikanie zakupu rozwiązań informatycznych pochodzących z krajów prowadzących nieprzychylną lub wrogą politykę wobec Rzeczypospolitej Polskiej, krajów objętych sankcjami Rady Bezpieczeństwa ONZ lub Unii Europejskiej oraz krajów wspierających terroryzm.
<b>DOKUMENTACJA SYSTEMU TELEINFORMATYCZNEGO</b>	
Dokumentacja Systemu Teleinformatycznego	System MUSI posiadać dokumentację – Dziennik Systemu Teleinformatycznego. Dokumentacja MUSI być aktualizowana w przypadku wprowadzania zmian w Systemie i być oznaczona w sposób jednoznaczny pozwalający określić do której wersji Systemu się odnosi
Dokumentacja Systemu Teleinformatycznego	Do dokumentacji Systemu MUSI być dołączona dokumentacja bezpieczeństwa. W dokumentacji bezpieczeństwa MUSZĄ być zamieszczone informacje na temat konfiguracji i mechanizmów w Systemie realizujących wymagania opisywane poniżej.
Dokumentacja Systemu Teleinformatycznego	Ogólny opis i relacje pomiędzy poszczególnymi komponentami Systemu (*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS): a. wyszczególnione segmenty sieci tzn. DMZ, strefa chroniona, Internet itp. oraz osadzenie tych komponentów w poszczególnych strefach, b. połączenia pomiędzy poszczególnymi komponentami, w tym: - usługi udostępniane pomiędzy poszczególnymi komponentami, - jaki protokół jest wykorzystywany w komunikacji, - numery portów dla usług w przypadku niestandardowej konfiguracji lub dla usług, które nie posiadają standardowego numeru portu, - który komponent w połączeniu inicjuje ruch, - w jaki sposób następuje uwierzytelnianie pomiędzy poszczególnymi komponentami, - w jaki sposób jest zachowana Integralność i Poufność w komunikacji.
Dokumentacja Systemu Teleinformatycznego	Opisane poszczególne komponenty w zakresie: a. mechanizmy tworzenia i odtwarzania kopii zapasowej z określonymi czasami trwania operacji (*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS), b. procedury przywracania po katastrofie (*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS), c. procedury aktualizacji oprogramowania (*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS), d. na jakich Kontach są uruchamiane usługi i z jakimi uprawnieniami (*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS), e. mechanizmy Kontroli stanu Systemu, f. w jaki sposób jest realizowany dostęp serwisowo-administracyjny (*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS), g. wykorzystywane Konta techniczne (*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS), h. zarządzanie Kontami w szczególności w zakresie ważności, wygasania, i. udostępniania zarządzania Kontami do zewnętrznego Systemu IAM, j. dostępnych metod uwierzytelniania Użytkowników i innych Systemów wchodzących w skład rozwiązania, k. polityki haseł lub innych środków uwierzytelnienia, l. zastosowanych mechanizmów autoryzacji Użytkowników i komponentów współpracujących, m. audytu działań i operacji w Systemie, n. wykorzystywanego mechanizmu logowania i możliwości podłączenia do zewnętrznego Systemu SIEM, o. mechanizmów synchronizacji czasu (*zapewnienia spójności danych w kontekście aktualnego czasu), p. zgodności z ustawą o ochronie danych osobowych.
<b>LOKALIZACJA, ŚRODOWISKO I ARCHITEKTURA</b>	
Lokalizacja, Środowisko I Architektura	System POWINIEN być fizycznie zlokalizowany w Centrum Przetwarzania Danych lub określonym środowisku chmurowym (ang. Cloud) potwierdzone na zgodność z wymaganiami ISO lub równoważnymi. Wymaganie nie dotyczy elementów Systemu w postaci stacji roboczych, urządzeń mobilnych korzystających z tego Systemu jako usługi.
Lokalizacja, Środowisko I Architektura	Normą ISO/IEC 27001:2023 Zarządzanie Bezpieczeństwem Informacji
Lokalizacja, Środowisko I Architektura	Normą ISO 22301 Zarządzanie Ciągłością Działania
Lokalizacja, Środowisko I Architektura	Normą ISO/IEC 27017 Bezpieczeństwo Informacji dla usług w Chmurze
Lokalizacja, Środowisko I Architektura	Normą ISO/IEC 27018 Ochrona Danych Osobowych w Chmurze
Lokalizacja, Środowisko I Architektura	Infrastruktura CPD/Cloud POWINNA gwarantować świadczenie usługi na zdefiniowanym poziomie SLA oraz być zlokalizowana geograficznie na terytorium Europejskiego Obszaru Gospodarczego
Lokalizacja, Środowisko I Architektura	Dla Systemów przetwarzających, w ocenie Zamawiającego, istotne dane (np. dane osobowe), MUSI być stosowane pełne szyfrowanie danych mocnymi algorytmami zarówno w spoczynku jak i w trakcie ich przesyłania.
Lokalizacja, Środowisko I Architektura	Dla Systemu MUSZĄ być opracowane procedury przywracania po katastrofie (*wymaganie nie dotyczy usług SaaS dla których istotne są parametry SLA oraz RTO/RPO oraz PCD).
Lokalizacja, Środowisko I Architektura	System POWINIEN posiadać co najmniej dwa środowiska: produkcyjne i testowe
Lokalizacja, Środowisko I Architektura	Dla Systemu MUSZĄ zostać zdefiniowane parametry RTO, RPO na okoliczność wystąpienia awarii usługi
Lokalizacja, Środowisko I Architektura	System NIE MOŻE posiadać pojedynczego punktu awarii („No Single Point of Failure”).
Lokalizacja, Środowisko I Architektura	System POWINIEN mieć dostępne mechanizmy tworzenia i odtwarzania kopii zapasowej z określonymi czasami trwania operacji.
<b>OPROGRAMOWANIE ORAZ KONTROLA STANU I ZMIAN W SYSTEMIE</b>	
Oprogramowanie Oraz Kontrola Stanu I Zmian W Systemie	System MUSI zapewniać mechanizmy umożliwiające aktualizację oprogramowania, w szczególności MUSI pozwalać na naprawę błędów związanych z bezpieczeństwem.
Oprogramowanie Oraz Kontrola Stanu I Zmian W Systemie	System MUSI posiadać mechanizmy kontroli i rejestracji zmian konfiguracji oraz aktualizacji oprogramowania.
Oprogramowanie Oraz Kontrola Stanu I Zmian W Systemie	Dla Systemu MUSI istnieć aktualna lista (w postaci załącznika do dokumentacji bezpieczeństwa) dostępnych aktualizacji bezpieczeństwa, które nie zostały wdrożone, z podanym uzasadnieniem.
Oprogramowanie Oraz Kontrola Stanu I Zmian W Systemie	System POWINIEN wykorzystywać tylko oprogramowanie w wersji wspieranej przez producenta.

Oprogramowanie Oraz Kontrola Stanu I Zmian W Systemie	Oprogramowanie POWINNO być uruchomione z minimalnymi uprawnieniami, które są konieczne do jego poprawnego funkcjonowania. W szczególności oprogramowanie NIE POWINNO być uruchamiane z uprawnieniami administratora (root'a).
Oprogramowanie Oraz Kontrola Stanu I Zmian W Systemie	W Systemie NIE POWINNO być zainstalowane oraz uruchomione oprogramowanie, które nie jest konieczne do jego poprawnego działania.
Oprogramowanie Oraz Kontrola Stanu I Zmian W Systemie	W Systemie POWINNY być wdrożone wszystkie udostępniane przez dostawców oprogramowania aktualizacje bezpieczeństwa dla wszystkich składników oprogramowania nie później niż 30 dni od daty ich udostępnienia.
Oprogramowanie Oraz Kontrola Stanu I Zmian W Systemie	W Systemie POWINNY być wdrożone mechanizmy do kontroli jego stanu. System MUSI posiadać mechanizmy automatycznego powiadamiania administratora o wystąpieniu błędu.
Oprogramowanie Oraz Kontrola Stanu I Zmian W Systemie	Wykorzystywane w Systemie oprogramowanie MUSI być autoryzowane, tzn. wolne od wirusów i malware, z potwierdzonymi prawami licencyjnymi
Oprogramowanie Oraz Kontrola Stanu I Zmian W Systemie	W przypadku udostępniania aplikacji mobilnej, MUSI być ona cyfrowo podpisana w celu umożliwienia jej identyfikacji, weryfikacji autentyczności i integralności
Oprogramowanie Oraz Kontrola Stanu I Zmian W Systemie	Treści wyświetlane na urządzeniach mobilnych powinny być „responsywne”, czyli powinny się dostosowywać automatycznie do wielkości ekranu
<b>RUCH SIECIOWY</b>	
Ruch Sieciowy	System POWINIEN być umieszczony w wydzielonym segmencie sieci fizycznej lub logicznej (VLAN).
Ruch Sieciowy	System MUSI udostępniać tylko usługi sieciowe niezbędne do jego działania lub obsługi serwisowo-administracyjnej.
Ruch Sieciowy	System MUSI mieć ściśle określony ruch sieciowy, tzn. zdefiniowane adresy do lub z innych segmentów sieci z którymi System się łączy. Ograniczenia ruchu MUSZĄ być zdefiniowane dla segmentu sieci jak i systemów operacyjnych wchodzących w skład Systemu.
Ruch Sieciowy	Dostęp serwisowo-administracyjny może być realizowany ze ściśle określonych adresów, rekomendowane jest wykorzystanie stacji przesiadkowych/zarządzających.
Ruch Sieciowy	Segment sieci wydzielony dla Systemu POWINIEN mieć adresację z jednej z klas adresowych zarezerwowanych dla prywatnych sieci lokalnych (RFC 1918/RFC4193).
Ruch Sieciowy	Komunikacja Systemu z innymi Systemami lub Użytkownikami POWINNA się odbywać za pomocą serwera pośredniczącego (Reverse Proxy). W przypadku ruchu przychodzącego z sieci niezaufanych ruch ten MUSI się odbywać za pomocą serwera pośredniczącego (Reverse Proxy).
Ruch Sieciowy	W przypadku komunikacji Systemu z innymi Systemami i Użytkownikami znajdującymi się w sieciach niezaufanych ruch musi odbywać się za pomocą elementu pośredniczącego umieszczonego w strefie DMZ.
Ruch Sieciowy	Wszystkie usługi Systemu MUSZĄ być w sieci jednoznacznie identyfikowane. Do identyfikacji ZALECANE jest wykorzystanie certyfikatów cyfrowych.
Ruch Sieciowy	Wymagany ruch sieciowy MUSI być opisany w sposób zgodny z wewnętrznym szablonem Zamawiającego.
Ruch Sieciowy	Ruch sieciowy przed przekazaniem do realizacji podlega procesowi kontroli zgodności z architekturą Systemu i akceptacji przez Zamawiającego.
Ruch Sieciowy	Szablon z ruchem sieciowym podlega wersjonowaniu i archiwizacji. POWINIEN być przechowywany w ustalonym pomiedzy zaangażowanymi w przygotowanie Systemu stronami wspólnym zasobie sieciowym, z właściwymi dla stron uprawnieniami (np. Sharepoint).
Ruch Sieciowy	Aktualny szablon z ruchem sieciowym służy jako wsad do dokumentacji technicznej Systemu oraz powykonawczej Dokumentacji Bezpieczeństwa
<b>KOMUNIKACJA</b>	
Komunikacja	Interfejsem używanym do komunikacji Użytkownika z Systemem POWINIEN być interfejs WWW.
Komunikacja	System do komunikacji z Użytkownikiem lub innym Systemem MUSI stosować połączenie zapewniające Integralność i Poufność przesyłanych danych.
Komunikacja	System do transmisji danych z zastosowaniem protokołu SSL/TLS POWINIEN stosować aktualne zalecenia NIST 800-131A, przykładowo: a. algorytm wymiany kluczy: DH/ECDE, RSA, b. algorytm uwierzytelniania: ECDSA, RSA c. długość klucza RSA co najmniej 2048, ECDSA co najmniej 256 d. symetryczny algorytm szyfrowania: AES-256 e. funkcje skrótu: SHA-2, SHA-256. f. rekomendowane użycie wersji TLS 1.3
Komunikacja	System do transmisji danych poprzez tunel VPN POWINIEN stosować protokół IPsec z parametrami uznanymi za obecnie dopuszczalne (nieprzestarzałe), np. opisane w NIST.SP.800-77 przykładowo: a. tryb pracy: ESP w trybie tunelowym, b. protokół negocjacji parametrów: IKE, c. metoda uwierzytelniania stron: certyfikaty cyfrowe, d. symetryczny algorytm szyfrowania: AES- 256 e. funkcje skrótu: SHA-2, SHA-256, f. grupa Diffie-Hellman: Group 19 lub wyższa, preferowana 24 g. tryb negocjacji w fazie I: Main mode, Aggressive mode (zabroniony), h. czas ważności kluczy: 3600 sekund.
Komunikacja	W Systemie MUSZĄ istnieć mechanizmy zapewniające kontrolę i walidację wprowadzanych danych.
Komunikacja	W przypadku wprowadzania ciągów znaków kontrola danych dotyczy ich formatu i składni lub udokumentowany brak podatności w tym zakresie.
Komunikacja	Wszystkie interfejsy dla danych wejściowych do Systemu MUSZĄ mieć zdefiniowane i zastosowane wzorce pozytywnej walidacji.
Komunikacja	Walidacja danych wejściowych do Systemu zakończona niepowodzeniem MUSI odrzucać lub oczyszczać przyjmowane dane.
Komunikacja	Wszystkie interfejsy dla danych wejściowych MUSZĄ posiadać zdefiniowaną stronę kodową np. UTF-8.
Komunikacja	Walidacja danych wejściowych MUSI się odbywać po stronie serwera.
Komunikacja	Wszystkie walidacje danych wejściowych zakończone niepowodzeniem POWINNY być logowane logowane lub udokumentowany brak podatności w tym zakresie.
Komunikacja	Usługa udostępniana po protokole http lub https MUSI być dostępna odpowiednio na portach 80 i 443 TCP. Dostęp do usługi na porcie HTTP MUSI automatycznie przekierowywać komunikację na port HTTPS.
Komunikacja	Dostęp do usługi musi wykorzystywać standardowe ustawienia komunikacji tcp/ip stosowane w ramach danego protokołu z uwzględnieniem zalecanych ustawień bezpiecznej komunikacji w ramach danego protokołu.(np. 3-way handshake do nawiązania sesji tcp, minimalne wersje SSL/TLS v.1.2, IPsecVPN w trybie MainMode) ) lub udokumentowany brak podatności w tym zakresie.
Komunikacja	Wymagane jest, aby usługa udostępniana poprzez https posiadała ważny certyfikat SSL wydany przez zaufany urząd certyfikacji
Komunikacja	Certyfikat wykorzystywany do uwierzytelnienia usługi musi być automatycznie rozpoznawany jako zaufany w systemach operacyjnych i przeglądarkach wykorzystywanych przez użytkowników

Komunikacja	W przypadku, gdy usługa udostępnia dane poprzez protokół http powinna ona działać na aktualnych i dopuszczonych przez Zamawiającego wersjach następujących przeglądarek internetowych, co najmniej: MS Edge, Mozilla FireFox ESR, Google Chrome.
<b>ZARZĄDZANIE UŻYTKOWNIKAMI</b>	
Zarządzanie Użytkownikami	System MUSI posiadać interfejs zarządzania uprawnieniami na potrzeby integracji z Systemem IAM, przeznaczonym do zarządzania tożsamością i uprawnieniami. Preferowanym standardem wymiany danych jest SPML. Dopuszczalne są także inne rodzaje interfejsów: a. SPMLv2 - DSMLv2 Profile udostępniony poprzez WebService, b. SPMLv2 – XSD Profile udostępniony poprzez WebService, c. DSMLv2 udostępniony poprzez WebService, d. LDAP, LDAP SSL e. dedykowane w Systemie WebService, f. dedykowane w Systemie API g. SSH.
Zarządzanie Użytkownikami	Interfejs dla Systemu IAM MUSI obejmować następujące funkcje związane z Kontami: a. utworzenie Konta, b. modyfikacja Konta, c. odczytanie informacji o Koncie, d. zablokowanie Konta, e. odblokowanie Konta, f. resetowanie haseł związanych z Kontem, g. usunięcie Konta – rozumiane jako trwałe zablokowanie dostępu do Konta, bez usuwania Identyfikatorów i historii operacji wykonanych przez Użytkownika danego Konta, h. przypisanie uprawnień do Konta, i. modyfikacja uprawnień przypisanych do Konta, j. odczytanie uprawnień przypisanych do Konta, k. odebranie uprawnień przypisanych do Konta, l. przekazanie listy wszystkich Kont.
Zarządzanie Użytkownikami	System musi posiadać zdefiniowaną i zaimplementowaną procedurę zarządzania kontami i uprawnieniami użytkowników usługi.
Zarządzanie Użytkownikami	W przypadku błędnego pięciokrotnego uwierzytelnienia użytkownika do usługi konto użytkownika MUSI być blokowane na pewien okres (np. 10 minut) lub należy zastosować inne mechanizmy ochrony (np. Capcha).
Zarządzanie Użytkownikami	Konta użytkowników wykorzystywane w usłudze muszą być imienne, tzn. niewspółdzielone.
Zarządzanie Użytkownikami	Usługa musi mieć zdefiniowaną procedurę resetu hasła dla kont nieobjętych funkcjonalnością SSO.
Zarządzanie Użytkownikami	Proces rejestracji nowych użytkowników i zakładania kont w Systemie musi uwzględniać mechanizmy do weryfikacji podawanych danych np. e-mail, wykluczenia robotów/automatów oraz wykorzystywać potwierdzenie osoby rejestrującej się za pośrednictwem bezpiecznych linków aktywacyjnych generowanych automatycznie i aktywnych przez określony, definiowalny okres czasu lub udokumentowany brak podatności w tym zakresie.
<b>KONTROLA DOSTĘPU</b>	
Kontrola Dostępu	Wszystkie Konta techniczne MUSZĄ być zewidencjonowane w dokumentacji bezpieczeństwa systemu. Wszystkie domyślne Hasła MUSZĄ zostać zmienione, a niewykorzystywane Konta zablokowane.
Kontrola Dostępu	System MUSI umożliwiać zdefiniowanie terminu wygasania ważności Konta Użytkownika.
Kontrola Dostępu	Po przekroczeniu daty wygasania, Konto MUSI być przez system automatycznie blokowane.
Kontrola Dostępu	System NIE POWINIEN umożliwiać usuwania Kont. Jeżeli w systemie jest taka funkcjonalność, POWINNA ona być zablokowana. Odnosnie danych osobowych powinny zostać zanonimizowane w dopuszczalnym zakresie.
Kontrola Dostępu	W Systemie MUSI istnieć funkcjonalność trwałego zablokowania Konta, uniemożliwiająca wykorzystanie Konta (zalogowanie się) nawet w przypadku posiadania prawidłowych danych uwierzytelniających.
Kontrola Dostępu	System MUSI mieć możliwość zaimplementowania mechanizmu powodującego zakończenie lub zablokowanie sesji w przypadku nieaktywności Użytkownika w określonym czasie. W przypadku sesji Administratora, zamykanie lub blokowanie sesji MUSI następować po 30 minutach nieaktywności.
Kontrola Dostępu	W Systemie, w którym istnieje ścieżka akceptacji (tzw. workflow) POWINNA istnieć funkcjonalność delegowania uprawnień lub wyznaczania zastępstw (eliminująca konieczność korzystania z Kont Użytkowników zastępowanych przez Użytkowników zastępujących).
Kontrola Dostępu	Lista Kont Technicznych MUSI zawierać informację o przeznaczeniu Konta (Konto Współdzielone lub Konto Serwisowe Interaktywne lub Nieinteraktywne) w celu późniejszej implementacji w Systemie PIM.
<b>UWIERZYTELNIANIE</b>	
Uwierzytelnianie	System MUSI zapewniać mechanizmy do uwierzytelniania Użytkowników oraz innych Systemów.
Uwierzytelnianie	System MUSI zapewniać Integralność i Poufność informacji o Kontach, w szczególności o Hasłach oraz innych danych w oparciu o które następuje uwierzytelnienie.
Uwierzytelnianie	System NIE MOŻE bez uwierzytelnienia udostępniać jakichkolwiek informacji lub funkcjonalności, które powinny być dostępne tylko po poprawnym uwierzytelnieniu.
Uwierzytelnianie	System POWINIEN uwierzytelniać Użytkownika przy pomocy jego Konta w domenie Zamawiającego. System do uwierzytelnienia Użytkownika POWINIEN korzystać z mechanizmu Kerberos lub NTLMv2 udostępnionych przez korporacyjne Active Directory lub stosować dopuszczalne metody uwierzytelniania bezhasłowego tzw. passwordless lub nowoczesnych metod uwierzytelniania SAML/ADFS wykorzystując zarazem funkcję jednokrotnego logowania tzw. SSO.
Uwierzytelnianie	System NIE POWINIEN wykorzystywać mechanizmów uwierzytelniania wymagających przesłania do Systemu Hasła Użytkownika. Zalecane jest wykorzystanie protokołu „Secure Remote Password” (RFC 2945/RFC 5054)
Uwierzytelnianie	System MUSI umożliwiać Użytkownikom, innym Systemom oraz administratorom zweryfikowanie autentyczności Systemu przed rozpoczęciem procedury uwierzytelniania (np. poprzez weryfikację certyfikatów X.509 serwera dla połączenia SSL, weryfikacji skrótu klucza publicznego serwera przy SSH itp.)
Uwierzytelnianie	Mechanizm interaktywnego wprowadzania Hasła lub numeru PIN przy uwierzytelnieniu do Systemu MUSI zapewnić Poufność wprowadzanych danych poprzez nie wyświetlanie ciągu wprowadzanych znaków.
Uwierzytelnianie	System MUSI wymuszać stosowanie przez Użytkowników trudnych Haseł, zgodnie z aktualnie stosowanymi najlepszymi praktykami, przykładowo minimalna długość hasła użytkownika 12 znaków, administratora 15 znaków lub stosować silne metody uwierzytelniania. W zakresie haseł dla Klientów Systemu (Użytkownik zewnętrzny), powinna być możliwość: - ustalenia odrębnych zasad niż dla użytkowników Zamawiającego; - wyłączenia wymuszenia zmiany hasła; - zastosowania komunikatu informującego o dobrych praktykach dotyczących haseł, zaleceniach jego zmiany i ryzyku związanym z zapamiętywaniem haseł na urządzeniach końcowych i w przeglądarkach (a w przypadku zapamiętywania, o potrzebie stosowania dodatkowych zabezpieczeń w dostępie do tych urządzeń: PIN/Hasło, odcisk palca itp.).
Uwierzytelnianie	System POWINIEN wymuszać na Użytkownikach okresowe zmiany Hasła dla kont nieobjętych SSO.

Uwierzytelnianie	W przypadku nieudanej próby uwierzytelnienia, System NIE MOŻE informować Użytkownika o tym, które wprowadzone przez niego dane są niepoprawne (powinien jedynie wyświetlić ogólny komunikat mówiący o nieudanym logowaniu, bez podania przyczyny).
Uwierzytelnianie	Po pierwszym udanym uwierzytelnieniu Użytkownika w Systemie, administracyjnym odblokowaniu konta, administracyjnej zmianie hasła, System POWINIEN wymusić zmianę Hasła przed udostępnieniem mu jakiegokolwiek innej funkcjonalności. Mechanizm wymuszania zmiany hasła powinien być możliwy do włączenia na koncie przez administratora dotyczy kont nietechnicznych oraz nieobietych SSO.
Uwierzytelnianie	System MUSI posiadać udokumentowane procedury zmiany haseł dla kont technicznych.
Uwierzytelnianie	System MUSI wspierać i udostępniać możliwość wykorzystania mechanizmów jednokrotnego uwierzytelniania SSO (Single Sign On) dla użytkowników wewnętrznych, uwierzytelniających się w korporacyjnej domenie Active Directory.
Uwierzytelnianie	System MUSI zapewniać mechanizmy pozwalające na zarządzanie danymi uwierzytelniającymi, tj. nadawaniem, zmianą, ponownym ustawieniem, czasem ważności.
Uwierzytelnianie	Dla każdego Użytkownika oraz innego Systemu MUSZĄ istnieć w Systemie dedykowane Konta.
Uwierzytelnianie	Hasła w Systemie POWINNY być przechowywane w postaci jednokierunkowych skrótów (ang. Hash) dla których zastosowano ciąg zaburzający (ang. salt).
Uwierzytelnianie	W przypadku uwierzytelniania Użytkowników na bazie certyfikatów PKI, mechanizm uwierzytelniania MUSI zapewniać: budowę i weryfikację pełnej ścieżki zaufania dla certyfikatu Użytkownika uwzględniając wytyczne standardu X.509, weryfikację ważności certyfikatu, weryfikację braku unieważnienia certyfikatu z aktualną w danej chwili listą CRL, weryfikację zgodności wystawcy z zaufanymi i autoryzowanymi wystawcami certyfikatów, istnienia powiązania certyfikatu z kontem w aplikacji oraz weryfikację podpisu cyfrowego użytkownika.
<b>AUTORYZACJA</b>	
Autoryzacja	System MUSI zapewniać mechanizmy do autoryzacji Użytkowników oraz innych Systemów.
Autoryzacja	System MUSI umożliwiać tworzenie Kont o różnych zakresach uprawnień. W szczególności System MUSI pozwalać na taką konfigurację uprawnień, aby Użytkownik lub inny System miał wyłącznie takie uprawnienia, jakie są mu niezbędne do wykonywania jego roli w Systemie.
Autoryzacja	Konta techniczne wykorzystywane w Systemie MUSZĄ mieć przyznany minimalny niezbędny zakres uprawnień.
Autoryzacja	System NIE POWINIEN udostępniać Użytkownikowi funkcjonalności polegającej na zadawaniu zapytań bezpośrednio do bazy danych. Dostęp do bazy danych MUSI być realizowany poprzez warstwę pośredniczącą separującą Użytkownika od bazy danych. Konto wykorzystywane przez warstwę pośredniczącą MUSI mieć ograniczone uprawnienia, tj. w szczególności NIE MOŻE być wykorzystywane w tym celu Konto Administratora bazy danych.
Autoryzacja	System POWINIEN umożliwiać przydzielanie uprawnień Użytkownikom pośrednio poprzez tworzenie grup Użytkowników i przydzielanie uprawnień grupom.
Autoryzacja	Dostęp do funkcji Systemu POWINIEN być zdefiniowany poprzez role w Systemie.
Autoryzacja	Wszystkie ustalone reguły kontroli dostępu do usług, funkcji, danych i obiektów MUSZĄ być wymuszane po stronie serwera.
Autoryzacja	Mechanizmy kontroli dostępu zaimplementowane w Systemie MUSZĄ utrzymywać aktualny stan uprawnień Użytkowników i w przypadku zmiany, ich egzekwowanie powinno być realizowane w trybie natychmiastowym.
Autoryzacja	Dostęp do Systemu zlokalizowanego poza infrastrukturą GK PGE POWINIEN umożliwiać stosowanie dodatkowego stopnia autoryzacji lub innego mechanizmu zabezpieczeń warunkującego dostęp.
<b>AUDYT DZIAŁAŃ I OPERACJI W SYSTEMIE</b>	
Audyt Działania I Operacji W Systemie	System MUSI posiadać mechanizmy do tworzenia i przechowywania audytu/logów (np. tabele logów, pliki logów) dotyczących działania Systemu.
Audyt Działania I Operacji W Systemie	Do audytu/logowania System POWINIEN wykorzystywać protokół Syslog. (*wymaganie nie dotyczy usług SaaS)
Audyt Działania I Operacji W Systemie	System MUSI zapewniać wsparcie dla audytu aktualizacji oprogramowania i zmian w konfiguracji. Zakres rejestrowanych informacji POWINIEN obejmować co najmniej: a. identyfikację obiektu lub komponentu, którego operacja dotyczy, b. czas operacji z dokładnością sekundy, c. Identyfikator Użytkownika wykonującego operację, d. adres IP, z którego wykonano operację, e. informację o pomyślnym zakończeniu operacji lub kodu zwróconego błędu w przypadku niepowodzenia.
Audyt Działania I Operacji W Systemie	W przypadku każdej (zarówno udanej jak i nieudanej) próby uwierzytelnienia System MUSI rejestrować następujące informacje: a. czas wykonania próby uwierzytelnienia z dokładnością sekundy, b. wprowadzony Identyfikator Użytkownika, c. adres IP, z którego wykonano próbę, d. rezultat procedury uwierzytelniania oraz autoryzacji (przyznanie lub odmowa dostępu z informacją o przyczynie odrzucenia).
Audyt Działania I Operacji W Systemie	W Systemie MUSI być określona lista typów działań Użytkownika, które podlegają rejestracji. Rejestrowane MUSZĄ być co najmniej następujące informacje: a. czas wykonania operacji z dokładnością sekundy, b. Identyfikator Użytkownika lub dane pozwalające na identyfikację Sesji Użytkownika, c. adres IP, z którego wykonano operację, d. kod, symbol lub pełny opis operacji wykonanej przez Użytkownika, e. obiekt lub komponent, którego operacja dotyczy, f. wszelkie argumenty lub dane użyte lub przekazane do Systemu podczas operacji, g. informacja o pomyślnym zakończeniu operacji lub kodu zwróconego błędu w przypadku niepowodzenia.
Audyt Działania I Operacji W Systemie	System MUSI mieć możliwość podłączenia do systemu SIEM. System MUSI mieć możliwość takiej konfiguracji, aby do Systemu SIEM mogły być logowane następujące informacje: a. błędy Systemu, b. operacje uwierzytelnienia (udane i nieudane), c. operacje nadawania i odbierania dostępu (MAC, RBAC, DAC), d. próby nieautoryzowanego dostępu do zasobów, e. informacje o możliwej awarii. f. otwarcie oraz zamknięcie – w tym automatyczne – sesji Użytkownika w Systemie g. zmiany w konfiguracji Systemu.
Audyt Działania I Operacji W Systemie	Preferowanym protokołem przekazywania zdarzeń do SIEM z systemów jest protokół Syslog (RFC 5424).
Audyt Działania I Operacji W Systemie	Usługa MUSI mieć włączone logowanie zdarzeń z retencją co najmniej 180 dni w zakresie a.operacji uwierzytelniania, poprawnego i niepoprawnego b.operacji nadawania i odbierania uprawnień c istotnych operacji w systemie związanych z działaniem użytkownika usługi d.operacji zablokowania konta w przypadku wielokrotnego błędnego uwierzytelnienia e.operacji resetu hasła



<b>SYNCHRONIZACJA CZASU</b>	
Synchronizacja Czasu	Wszystkie komponenty Systemu MUSZĄ być synchronizowane ze wspólnym wzorcem czasu, którego rolę pełni dedykowany do tego celu serwer czasu. ZABRONIONE jest synchronizowanie czasu ze źródeł zewnętrznych i serwerów do tego nieprzeznaczonych. Systemy operacyjne Microsoft Windows będące członkami domeny GK PGE MOGA <u>wykorzystywać kontrolery domeny jako źródło czasu.</u>
Synchronizacja Czasu	Synchronizacja czasu dla wszystkich komponentów Systemu POWINNA odbywać się przy pomocy protokołu Network Time Protocol (NTP) lub Simple Network Time Protocol (SNTP).
<b>ZGODNOŚĆ Z PRZEPISAMI PRAWA</b>	
Zgodność Z Przepisami Prawa	Jeżeli w Systemie przetwarzane są Dane Osobowe to MUSI być on zgodny z przepisami o ochronie danych osobowych, a w szczególności: a.Zapewnić możliwość realizacja Praw jednostki dla Danych Osobowych przetwarzanych w tym systemie, w tym: i.Prawo dostępu (i uzyskania kopii danych) – Art. 15 RODO ii.Prawo do sprostowania danych - Art. 16 RODO iii.Prawo do usunięcia danych ("prawo do bycia zapomnianym") – ART.17 RODO iv.Prawo do ograniczenia przetwarzania – Art. 18 RODO v.Prawo do przenoszenia danych – Art. 20 RODO vi.Prawo do sprzeciwu – Art. 21 RODO b.Zapewnić spełnianie wymogu Minimalizacja danych, czyli: i.Przetwarzamy tylko dane niezbędne do realizacji celu przetwarzania ii.Przetwarzamy dane tylko przez okres uzasadniony celem przetwarzania. Należy zapewnić możliwość usuwania z systemu danych, gdy wygasa podstawa przetwarzania - dla wszystkich instancji danych (produkcyjne, testowe, logi, kopie zapasowe, archiwa, itp.)
<b>Kryptografia</b>	Dopuszczalne są standardy kryptograficzne (symetryczne, asymetryczne, podpisu cyfrowego) aktualnie uznane za rekomendowane (nieprzestarzałe), np. w oparciu o publikację NIST.SP.800-175B:
Kryptografia	Dopuszczalne są następujące standardy szyfrowania symetrycznego: Algorytm : Długość klucza AES : 256 bitów i więcej Twofish : 256 bitów i więcej IDEA : 256 bitów CHACHA20 : 256 bitów i więcej Zalecane tryby to GCM, CFB, OFB, CTR, CBC z wykorzystaniem wektora inicjalizującego (IV – Initialization Vector) generowanego za każdym razem z zachowaniem poufności.
Kryptografia	Dopuszczalne są następujące standardy szyfrowania asymetrycznego: Algorytm : Długość klucza RSA : 2048 bitów i więcej ECC : 256 bitów i więcej
Kryptografia	Dopuszczalne są następujące standardy wyciszania skrótów: Algorytm : SHA-2 SHA-3 RIPEMD-160
Kryptografia	Dopuszczalne są następujące standardy MAC (Message Authentication Code): Algorytm : HMAC CBC-MAC CMAC POLY1305
Kryptografia	Dopuszczalne są następujące standardy podpisu cyfrowego: Algorytm : Długość klucza RSA : 2048 bitów i więcej ECDSA : 256 bitów i więcej DSA : 2048 bitów i więcej
<b>WYMAGANIA SZCZEGÓLNE WZGLĘDEM SYSTEMÓW BĘDĄCYCH APLIKACJAMI WEBOWYMI</b>	
Aplikacje webowe	Tworzone aplikacje webowe MUSZĄ być wolne od podatności i błędów identyfikowanych jako 10 najczęstszych według aktualnej listy OWASP TOP 10.
Aplikacje webowe	Niezależnie od aktualnej zawartości listy OWASP TOP 10 aplikacje webowe MUSZĄ być wolne od następujących podatności i błędów: (a)Injection - możliwości wstrzykiwania nieautoryzowanych komend w przekazywanych parametrach do aplikacji, (b)Broken Authentication and Session Management - możliwości przechwytywania haseł oraz identyfikatorów sesji, zarówno podczas transmisji oraz ich przechowywania, (c)Cross Site Scripting (XSS) – możliwości osadzenia kodu w treści atakowanej strony, (d)Insecure Direct Object References – możliwości bezpośredniego nieautoryzowanego odwoływania się do obiektów poprzez modyfikację parametrów, (e)Security Misconfiguration - błędów w konfiguracji w postaci: i.braków w aktualizacji komponentów, ii.niewyłączenia nieużywanych usług, kont, stron, portów, iii.braku zamiany domyślnych haseł, iv.wyświetlania kodu błędów oraz stosu wywołań w przypadku wystąpienia błędu aplikacji, (f)Sensitive Data Exposure – podatności w przetwarzaniu danych wrażliwych w postaci: i. przesyłania danych w postaci jawnej, ii. przechowywania danych w postaci jawnej, iii. używania słabych algorytmów kryptograficznych, iv słabych – krótkich – kluczy kryptograficznych, v. nieodpowiedniego zarządzania kluczami kryptograficznymi, (g)Missing Function Level Access Control – błędów w aplikacji w postaci: i.braku ograniczenia dostępu w przypadku nieuwierzytelniania, ii.braku ograniczenia dostępu do zasobów zawierających dane konfiguracyjne, logi zdarzeń, pliki źródłowe, iii.braku ograniczenia dostępu do zasobów w zależności od uprawnień, (h)Cross-Site Request Forgery (CSRF) – możliwości przesyłania natyryzowanych żądań do aplikacji, (i)Using Components with Known Vulnerabilities – używania komponentów, modułów i bibliotek ze znanymi podatnościami, (j)Unvalidated Redirects and Forwards – braku walidacji parametrów zawierających adresy przekierowania i przeniesienia.
Aplikacje webowe	Wykonanie wrażliwych operacji w aplikacji POWINNO być poprzedzone ponownym uwierzytelnieniem.
Aplikacje webowe	Wszystkie strony oraz zasoby MUSZĄ wymagać uwierzytelnienia za wyjątkiem tych specjalnie przeznaczonych dla dostępu publicznego.

Aplikacje webowe	Aplikacja webowa MUSI zapewniać mechanizmy zapewniające kontrolę sesji uwierzytelnionego Użytkownika poprzez stosowanie unikalnego identyfikatora. Względem Identyfikatora sesji są następujące wymagania: (a)NIE MOŻE być krótszy niż 128 bitów, (b)MUSI być losowy, (c)MUSI być generowany z jak najszerzego zestawu znaków, (d)MUSI być unikatowy dla Użytkowników danej aplikacji, (e)MUSI być zmieniany/generowany przy uwierzytelnieniu Użytkownika, (f)MUSI być zmieniany/deaktywowany przy wylogowaniu Użytkownika (g)MUSI być zmieniany/generowany przy przejściu pomiędzy HTTP i HTTPS, (h)POWINIEN być akceptowany za poprawny tylko ten identyfikator, który został wygenerowany przez aplikację, (i)MUSI być unieważniany po określonym czasie bezczynności Użytkownika, (j)MUSI być przekazywany poprzez nagłówek cookie, w szczególności NIE MOŻE być przekazywany w adresie URL. Wlicza się w to wyłączenie wsparcia dla tzw. „URL rewriting” dla ciasteczek sesyjnych, (k)NIE MOŻE być ujawniany w komunikatach błędów i logach, (l)MUSI być unieważniany i zmieniany lub usuwany przy wylogowaniu Użytkownika, (m)NIE MOŻE być zapamiętywany w przeglądarce (brak funkcji zapamiętaj mnie), (n)Cookie zawierające uwierzytelnione identyfikatory sesji MUSZĄ mieć ustawione atrybuty domain i path odpowiednio dla lokalizacji.
Aplikacje webowe	W przypadku, gdy aplikacja zawiera strony lub zasoby wymagające uwierzytelnienia, to MUSI być zaimplementowany mechanizm w postaci linków lub przycisków, pozwalający Użytkownikowi w sposób jasny i świadomy wybranie operacji uwierzytelnienia w aplikacji oraz operacji wylogowania się z aplikacji. Po wylogowaniu się z aplikacji Użytkownik MUSI być przekierowany do strony w aplikacji nie wymagającej uwierzytelnienia.
Aplikacje webowe	Dla Cookie sesyjnych MUSZĄ być ustawione opcje Secure oraz HttpOnly. (więcej informacji: <a href="https://sekurak.pl/flaga-cookie-httponly/">https://sekurak.pl/flaga-cookie-httponly/</a> )
Aplikacje webowe	Dane uwierzytelniające NIE MOGĄ być przekazywane w parametrach adresu URL.
Aplikacje webowe	Aplikacja MUSI posiadać mechanizm ochrony przez atakami siłowymi (ang. brute-force) na dane uwierzytelniające, blokujący kolejne próby uwierzytelnienia na zdefiniowany okres czasu. Blokada POWINNA dotyczyć zarówno adresu źródłowego jak i Konta. Blokowanie możliwości uwierzytelnienia dla danego Konta POWINNO następować po 5 nieudanych próbach, po 3 nieudanej próbie powinny być zastosowane mechanizmy wykluczające automaty (np. Capcha). Okres blokowania POWINIEN trwać minimum 15 minut, a licznik blokowania możliwości uwierzytelnienia dla Konta POWINIEN być zerowany po 5 minutach. Aplikacja POWINNA posiadać mechanizm pozwalający na bezwzględne blokowanie możliwości uwierzytelnienia dla Konta, po przekroczeniu ustalonej liczby nieudanych prób uwierzytelnienia.
Aplikacje webowe	Pola służące do wprowadzania Hasła MUSZĄ mieć wyłączoną funkcję automatycznego uzupełnienia i zapamiętywania – dla Użytkowników Zamawiającego i GK PGE. Dopuszczalne jest zapamiętywanie haseł przez Klientów jeżeli jest to uzasadnione funkcjonalnie.
Aplikacje webowe	Udostępniane przez aplikację strony MUSZĄ mieć zdefiniowany nagłówek Content Security Policy zawierający co najmniej dyrektywę default-src oraz jeżeli to konieczne dyrektywy script-src, img-src, frame-src, connect-src. Dyrektywy te POWINNY zezwalać jedynie na połączenia do domeny z której jest serwowana dana strona tzn. mieć ustawioną wartość 'self'.
Aplikacje webowe	Udostępniane przez aplikację strony MUSZĄ mieć zdefiniowany nagłówek X-XSS-Protection. Nagłówek MUSI mieć następującą postać: X-XSS-Protection: 1; mode=block; a)wartość 1 pozwala na filtrowanie ze względu na XSS, b)wartość mode=block pozwala na blokowanie przez przeglądarkę wykonanie kodu w przypadku wykrycia podejrzanego skryptu (*wymaganie uchylone, niestosowane w nowoczesnych przeglądarkach).
Aplikacje webowe	Udostępniane przez aplikację po HTTPS strony MUSZĄ mieć zdefiniowany nagłówek Strict-Transport-Security. Nagłówek POWINIEN mieć następującą postać: Strict-Transport-Security: max-age=31536000; includeSubDomains (a)wartość max-age=31536000 wymusza, że wszelkie zapytania w przyszłości określonej przez max-age do danej witryny muszą odbywać się po HTTPS, (b)wartość includeSubDomains wymusza, że wszystkie odwołania na stronie i poddomenach zamieniane są na odwołania po HTTPS.
Aplikacje webowe	Aplikacja POWINNA dla zapytań HTTP dopuszczać jedynie metody GET oraz POST lub posiadać udokumentowany brak podatności w tym zakresie.
Aplikacje webowe	Wysyłane pliki od Użytkownika do aplikacji POWINNY być sprawdzane pod względem zawartości złośliwego kodu. System MUSI dopuszczać zaimportowanie wyłącznie określone kategorie plików.
Aplikacje webowe	Przekazywane do aplikacji parametry dotyczące odwołań do plików MUSZĄ podlegać sprawdzaniu w celu uniknięcia ataków manipulujących ścieżką tzw. path traversal.
Aplikacje webowe	Wszystkie dane przesyłane do aplikacji, których wynikiem jest kod HTML (elementy HTML, atrybuty HTML, wartości danych javascript, bloki CSS i atrybuty URI) MUSZĄ podlegać escapowaniu odpowiednio do kontekstu. Wszystkie mechanizmy enkodowania / escapowania muszą być zaimplementowane po stronie serwera.
Aplikacje webowe	Aplikacja NIE POWINNA wymagać instalacji w przeglądarce internetowej dodatkowych komponentów typu ActiveX, aplet Java.
Aplikacje webowe	Aplikacja NIE POWINNA korzystać z komponentów Adobe Flash, Microsoft Silverlight.
<b>WYMAGANIA SZCZEGÓLNE DLA SYSTEMU ULOKOWANEGO W CHMURZE PUBLICZNEJ W MODELU IaaS/FaaS/PaaS/SaaS NADZOROWANEJ PRZEZ DOSTAWCĘ</b>	
Zgodność z normami	Wymagane jest posiadanie certyfikacji potwierdzających zgodność z: (a)Normą ISO/IEC 27001:2023 Zarządzanie Bezpieczeństwem Informacji (b)Normą ISO 22301 Zarządzanie Ciągłością Działania (c)Normą ISO 27017 Bezpieczeństwo Informacji dla usług w Chmurze (d)Normą ISO 27018 Ochrona Danych Osobowych w Chmurze (e)Norma ISO 27701 Zarządzanie i ochrona danych osobowych w chmurze obliczeniowej
Najlepsze praktyki i niezależne certyfikacje	Wymagane jest wykorzystanie przez Dostawcę najlepszych praktyk branżowych: (a)CSA – ang. Cloud Security Alliance certyfikacja STAR ang. Security Trust Assurance and Risk ( <a href="https://www.bsigroup.com/pl-PL/Certyfikacja-CSA-STAR/">https://www.bsigroup.com/pl-PL/Certyfikacja-CSA-STAR/</a> ). Wymagane jest zapewnienie przez Dostawcę raportu potwierdzającego zgodność zabezpieczeń z aktualną macierzą kontroli (ang. CSA CCM Self-Assessment). (b)CIS – ang. Center for Internet Security (zalecenia kontrolne/benchmarki, utwardzanie systemów, w szczególności dla rozwiązań chmurowych „CIS Cloud Companion”) (c)OWASP – ang. Open Web Application Security Project (d)ASVS – ang. Application Security Verification Standard (standardowo Level 2, natomiast gdy dotyczy infrastruktury krytycznej – Level 3)
Dedykowane chmurze obliczeniowej	System MUSI być zgodny z RODO a przetwarzanie danych odbywa się w granicach EOG (Europejskiego Obszaru Gospodarczego)

Dedykowane chmurze obliczeniowej	Preferowane są lokalizacje przetwarzania danych na terytorium Polski
Dedykowane chmurze obliczeniowej	Dostawca chmury oraz usług w chmurze w każdym aspekcie dostępu do zasobów POWINIEN dokładać wszelkich najlepszych starań, aby zapewnić danym/informacji: poufność, integralność, dostępność oraz rozliczalność. Zarówno w obszarach przechowywania danych, jak i podczas ich transportu pomiędzy różnymi środowiskami „Systemu” lub integracji z innymi „Systemami”. Należyta dokładność POWINNA być stosowana już na etapie analizy rozwiązań chmurowych, jak i w trakcie projektowania oraz realizacji rozwiązań.
Dedykowane chmurze obliczeniowej	System MUSI wspierać sposób uwierzytelnienia przez ADFS Zamawiającego lub Azure AD/Entra ID.
Dedykowane chmurze obliczeniowej	System MUSI umożliwiać skonfigurowanie uwierzytelnienia 2 Factor Authentication (uwierzytelnianie 2 składnikowe)
Dedykowane chmurze obliczeniowej	Wymagane jest dopuszczenie możliwości przeprowadzenia szczegółowego audytu dla usług dostarczanych poza infrastrukturą zamawiającego.
Dedykowane chmurze obliczeniowej	Wymagane jest spełnienie oczekiwanego SLA w szczególności brak pojedynczego punktu awarii oraz odpowiednia odporność na awarie komponentów chmurowych.
Dedykowane chmurze obliczeniowej	Wymagane jest wykorzystanie mechanizmów ochrony sieciowej (Firewall, WAF, DDoS) dla usług udostępnianych publicznie oraz przeprowadzenia testów penetracyjnych, w szczególności zabezpieczenia aplikacji webowych, przed udostępnieniem produkcyjnym. Udostępnienie Systemu publicznie MOŻE być zrealizowane po wyeliminowaniu ujawnionych podatności.
Dedykowane chmurze obliczeniowej	Dla usług niewymagających dostępu publicznego wymaga się wykorzystania dostępu warunkowego dopuszczającego dostęp do usługi wyłącznie z infrastruktury Zamawiającego w uzgodniony optymalny sposób, np.: (a)Filtrowanie ruchu IP na zaporach sieciowych (b)Zastosowanie tunelowania IPSec VPN pomiędzy CPD Zamawiającego a środowiskiem chmurowym (c)Zastosowanie minimum 2FA/MFA w przypadku braku innych możliwości
Dedykowane chmurze obliczeniowej	Preferowane jest wykorzystanie uniwersalnej warstwy abstrakcji niezależniającej się od dostawcy chmury, np.: (a)Zastosowanie konteneryzacji (b)Zastosowanie wirtualizacji VMWare on Cloud (c)Wsparcie dla oprogramowania firm trzecich przeprowadzających migrację pomiędzy dostawcami chmur obliczeniowych (d)Zastosowanie w Systemie funkcjonalności IaC ang. Infrastructure as a Code
Dedykowane chmurze obliczeniowej	Wymagane jest przygotowanie planu wyjścia z usługi chmurowej na wypadek awarii lub nagłego zaprzestania świadczenia usług przez dostawcę chmury (migracja Systemu do innego dostawcy chmury lub środowiska Zamawiającego)
<b>WYMAGANIA DEDYKOWANE DO REALIZACJI PRZEZ DOSTAWCĘ NA ETAPIE WDROŻENIA</b>	
Dedykowane chmurze obliczeniowej	Opracowanie przedwdrożeniowej dokumentacji technicznej Systemu w konsultacji z Architektem bezpieczeństwa oraz Cyberbezpieczeństwa Zamawiającego (*wymagane dotyczy udokumentowania komponentów odpowiednio dla standardu modelu odpowiedzialności dla usług chmurowych CSP/Wykonawca/Zamawiający)
Dedykowane chmurze obliczeniowej	Uruchomienie uwierzytelniania dwuskładnikowego (2FA) do usług chmurowych (dostęp typu back office) z udziałem ADFS Zamawiającego jako IDP (ang. Identity Provider) i stosowanymi mechanizmami jednokrotnego logowania SSO
Dedykowane chmurze obliczeniowej	Wykorzystanie w procesie nadawania uprawnień systemu IAM Zamawiającego
Dedykowane chmurze obliczeniowej	Wymagane jest przesyłanie incydentów i zdarzeń bezpieczeństwa do systemów Zamawiającego (rekomendowana integracja zdarzeń po stronie chmury z systemami Zamawiającego SIEM/SOAR).
Dedykowane chmurze obliczeniowej	Zapewnienie odrębnej kopii zapasowej danych Systemu w infrastrukturze Zamawiającego (np. integracja z systemem kopii zapasowych Zamawiającego lub okresowe automatyczne eksporty danych)
Dedykowane chmurze obliczeniowej	Wymaga się opracowania, udokumentowania i przetestowania planu wycofania Systemu z usług chmury obliczeniowej (również na wypadek awarii), bez uszczerbku dla zachowania zgodności działania z wymaganiami prawa i innych regulacji, w tym w szczególności związanych z udzielonymi licencjami lub zezwoleniami. Plan może zakładać wykorzystanie środowiska „on-premises”, migrację do innego dostawcy lub inne scenariusze biznesowe.
Dedykowane chmurze obliczeniowej	Przekazanie niezbędnych kompetencji (szkoleń) zespołowi PGE-CERT w kontekście analizy i reagowania na incydenty bezpieczeństwa w zakresie Systemu po stronie usług chmury obliczeniowej.
<b>ZGŁASZANIE INCYDENTÓW BEZPIECZEŃSTWA</b>	
ZGŁASZANIE INCYDENTÓW BEZPIECZEŃSTWA	Dostawca zobowiązany jest do bezzwrotnego informowania Zamawiającego o: 1.18.1.1. zauważonym przypadku naruszenia bezpieczeństwa systemów i zasobów teleinformatycznych, mających wpływ lub będących w zakresie świadczonych usług 1.18.1.2. wykryciu podatności lub luki w zabezpieczeniach usług/Systemu, 1.18.1.3. stwierdzonym przypadku naruszenia integralności sprzętu, oprogramowania bądź podejrzeniu próby takiego naruszenia, 1.18.1.4. stwierdzonym przypadku infekcji szkodliwym oprogramowaniem stacji roboczej, z której inicjowany jest dostęp do usługi/Systemu, 1.18.1.5. podejrzeniu utraty poufności indywidualnych danych uwierzytelniających
ZGŁASZANIE INCYDENTÓW BEZPIECZEŃSTWA	Dostawca zobowiązuje się do informowania Zamawiającego o wykrytych incydentach bezpieczeństwa dot. danych powierzonych do przetwarzania przez Zamawiającego (np. wielokrotne nieudane próby logowania, lub wykrycie złośliwej zawartości) oraz o atakach na systemy inne Wykonawcy, gdy używa infrastruktury połączonej z Zamawiającym (skomunikowanej z innymi usługami Zamawiającego)