

Załącznik 4 – Wymagania bezpieczeństwa - Tabela

Grupa wymagań	Opis
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 po akceptacji odstępstwa przez Zamawiającego.
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.
Dokumentacja Systemu Teleinformatycznego	Każdy 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 (dotyczy to również dostępu Wykonawcy do środowisk PrePROD i Dev).
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 zamieszczone w niniejszej Procedurze.
Dokumentacja Systemu Teleinformatycznego	Ogólny opis i relacje pomiędzy poszczególnymi komponentami Systemu: 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, b. procedury przywracania po katastrofie, c. procedury aktualizacji oprogramowania, d. na jakich Kontach są uruchamiane usługi i z jakimi uprawnieniami, e. mechanizmy Kontroli stanu Systemu, f. w jaki sposób jest realizowany dostęp serwisowo-administracyjny, g. wykorzystywane Konta techniczne, 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, p. zgodności z ustawą o ochronie danych osobowych.

Lokalizacja, Środowisko I Architektura	System MUSI być fizycznie zlokalizowany w Centrum Przetwarzania Danych. Wymaganie nie dotyczy elementów Systemu w postaci stacji roboczych, urządzeń mobilnych korzystających z tego Systemu jako usługi.
Lokalizacja, Środowisko I Architektura	Infrastruktura CPD MUSI gwarantować świadczenie usługi na zdefiniowanym poziomie SLA
Lokalizacja, Środowisko I Architektura	System MUSI być wolny od pojedynczego punktu awarii („No Single Point of Failure”).
Lokalizacja, Środowisko I Architektura	System MUSI mieć dostępne mechanizmy tworzenia i odtwarzania kopii zapasowej z określonymi czasami trwania operacji.
Lokalizacja, Środowisko I Architektura	Dla Systemu MUSI być stosowane pełne szyfrowanie danych mocnymi algorytmami baz danych przechowujących te dane zgodnie z wymaganiami kryptograficznymi opisanymi poniżej.
Lokalizacja, Środowisko I Architektura	Dla Systemu MUSZĄ być opracowane procedury przywracania po katastrofie.
Lokalizacja, Środowisko I Architektura	System MUSI 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
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 zintegrowane mechanizmy kontroli i rejestracji zmian konfiguracji oraz aktualizacji oprogramowania pozwalające na przegląd wprowadzonych zmian.
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 dostarczanego 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 przez Dostawcę zweryfikowane, tzn. wolne od wirusów i malware, z potwierdzonymi prawami licencyjnymi i wspierane przez Dostawcę w trakcie okresu utrzymania

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
Ruch Sieciowy	System oraz oddzielne subkomponenty (np.. TEST, PROD) POWINNY być umieszczone 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 MUSI 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 w przypadku ruchu przychodzącego do Systemu POWINNA się odbywać za pomocą serwera pośredniczącego (Reverse Proxy). W przypadku ruchu przychodzącego z sieci niezauważanych 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 niezauważanych ruch MUSI odbywać się za pomocą elementu pośredniczącego umieszczonego w strefie DMZ.
Ruch Sieciowy	Wszystkie komponenty Systemu MUSZĄ być w sieci jednoznacznie identyfikowane. Do identyfikacji ZALECANE jest wykorzystanie certyfikatów cyfrowych.
Ruch Sieciowy	Wymagany ruch sieciowy MUSI być opisany w sposób przedstawiony w Zał.1 do PROC 55036 - Opis ruchu sieciowego - przykłady .Ruch sieciowy przed przekazaniem do realizacji podlega procesowi kontroli zgodności z architekturą Systemu i akceptacji od strony bezpieczeństwa
Ruch Sieciowy	Załącznik 1 z ruchem sieciowym podlega wersjonowaniu i archiwizacji. POWINIEN być przechowywany w ustalonym pomiędzy zaangażowanymi w przygotowanie Systemu stronami wspólnym zasobie sieciowym, z właściwymi dla stron uprawnieniami (np. Sharepoint). Aktualny Załącznik 1 służy jako wsad do dokumentacji technicznej Systemu oraz powykonawczej Dokumentacji Bezpieczeństwa
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 w tym HTTPS POWINIEN stosować wyłącznie protokół TLS v1.2 (lub wyżej, z koniecznością wyłączenia kompresji TLS i negocjacji niższych wersji) z następującymi parametrami: a. algorytm wymiany kluczy: RSA, Diffie-Hellman (RSA), b. algorytm uwierzytelniania: RSA, c. długość klucza RSA co najmniej 2048, d. symetryczny algorytm szyfrowania: AES-256 (preferowany) e. funkcje skrótu: SHA-2, SHA-256 (preferowana).

Komunikacja	System do transmisji danych poprzez tunel VPN POWINIEN stosować protokół IPSec z następującymi parametrami: a. tryb pracy: ESP w trybie tunelowym, b. protokół negocjacji parametrów: IKE, c. metoda uwierzytelniania stron: certyfikaty cyfrowe, d. symetryczny algorytm szyfrowania: AES- 256(preferowany) e. funkcje skrótu: SHA-2, SHA-256 (preferowana), f. grupa Diffie-Hellman: Group 15 lub wyższa, preferowana 19 lub 24 g. tryb negocjacji w fazie I: Main mode, Aggresive mode (zabroniony), h. czas ważności kluczy: 3600 sekund.
Komunikacja	W Systemie MUSZĄ istnieć mechanizmy zapewniające kontrolę i walidację wprowadzanych danych.
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 rejestrowane w pliku logów.
Komunikacja	Usługa udostępniana po protokole http lub https MUSI być dostępna odpowiednio na portach 80 i 443
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)
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/s powinna ona działać na aktualnych i dopuszczonych przez Zamawiającego wersjach następujących przeglądarek internetowych: MS Edge, Mozilla FireFox, Google Chrome
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	<p>Interfejs dla Systemu IAM MUSI obejmować następujące funkcje związane z Kontami:</p> <ul style="list-style-type: none"> <li>a. utworzenie Konta,</li> <li>b. modyfikacja Konta,</li> <li>c. odczytanie informacji o Koncie,</li> <li>d. zablokowanie Konta,</li> <li>e. odblokowanie Konta,</li> <li>f. resetowanie haseł związanych z Kontem,</li> <li>g. usunięcie Konta – rozumiane jako trwałe zablokowanie dostępu do Konta, bez usuwania Identyfikatorów i historii operacji wykonanych przez Użytkownika danego Konta,</li> <li>h. przypisanie uprawnień do Konta,</li> <li>i. modyfikacja uprawnień przypisanych do Konta,</li> <li>j. odczytanie uprawnień przypisanych do Konta,</li> <li>k. odebranie uprawnień przypisanych do Konta,</li> <li>l. przekazanie listy wszystkich Kont.</li> </ul>
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 MOŻE umożliwiać usuwania Kont. Jeżeli w systemie jest taka funkcjonalność, MUSI ona być zablokowana. Odnośnie 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.
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 GKPGE (gkpge.pl). System do uwierzytelnienia Użytkownika POWINIEN korzystać z mechanizmu Kerberos lub NTLMv2 udostępnionych przez korporacyjne Active Directory. Nie dotyczy to klientów zewnętrznych Spółki.
Uwierzytelnianie	System NIE MOŻE wykorzystywać mechanizmów uwierzytelniania wymagających przesłania do Systemu Hasła Użytkownika.

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	System NIE MOŻE wyświetlać w sposób czytelny (np. na ekranie monitora itp.) wprowadzanych Haseł lub numerów PIN.
Uwierzytelnianie	System MUSI wymuszać stosowanie przez Użytkowników trudnych Haseł lub wykorzystywać silne metody uwierzytelniania.
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 nieobjętych 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. Odstępstwem od wymagania są Konta techniczne.
Uwierzytelnianie	Hasła w Systemie MUSZĄ 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.
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 MUSI 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.
Audyt Działań I Operacji W Systemie	System MUSI posiadać mechanizmy do tworzenia i przechowywania audytu/logów (np. tabele logów, pliki logów) dotyczących działania Systemu.
Audyt Działań I Operacji W Systemie	Do audytu/logowania System POWINIEN wykorzystywać protokół Syslog.
Audyt Działań 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 nie mniejszą niż 1 sekunda, c. Identyfikator Użytkownika wykonującego operację, d. adres IP, z którego wykonano operację, e. informację o pomyślnym zakończeniu operacji lub kod zwróconego błędu w przypadku niepowodzenia.
Audyt Działań 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 nie mniejszą niż 1 sekunda, 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 Działań 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 nie mniejszą niż 1 sekunda, 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 Działań 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 Działów I Operacji W Systemie	Preferowanym protokołem przekazywania zdarzeń do SIEM z systemów jest protokół Syslog (RFC 5424).
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 wykorzystywać kontrolery domeny jako źródło czasu.
Synchronizacja Czasu	Synchronizacja czasu dla wszystkich komponentów Systemu POWINNA odbywać się przy pomocy protokołu Network Time Protocol (NTP) lub Simple Network Time Protocol (SNTP).
Zgodność Z Przepisami Prawa	<p>Jeżeli w Systemie przetwarzane są Dane Osobowe to MUSI być on zgodny z przepisami o ochronie danych osobowych, a w szczególności:</p> <p>a. Zapewnić możliwość realizacja Praw jednostki dla Danych Osobowych przetwarzanych w tym systemie, czyli:</p> <ul style="list-style-type: none"> <li>i. Obowiązek informacyjny (wobec osób fizycznych oraz osób prowadzących działalność gospodarczą) Art.13 i 14 RODO.</li> <li>ii. Prawo dostępu (i uzyskania kopii danych) – Art. 15 RODO</li> <li>iii. Prawo do sprostowania danych - Art. 16 RODO</li> <li>iv. Prawo do usunięcia danych ("prawo do bycia zapomnianym") – ART.17</li> <li>v. Prawo do ograniczenia przetwarzania – Art. 18</li> <li>vi. Prawo do przenoszenia danych – Art. 20</li> <li>vii. Prawo do sprzeciwu – Art. 21 i Art. 22b.</li> </ul> <p>b. Zapewnić spełnianie wymogu Minimalizacja, czyli:</p> <ul style="list-style-type: none"> <li>i. Przetwarzamy tylko dane niezbędne do realizacji celu przetwarzania</li> <li>ii. Przetwarzamy dane tylko przez okres uzasadniony celem przetwarzania. Należy zapewnić możliwość usuwania z systemu danych, gdy wygasła podstawa przetwarzania - dla wszystkich instancji danych (produkcyjne, testowe, logi, kopie zapasowe, archiwa, itp.)</li> </ul>
Kryptografia	<p>Dopuszczalne są następujące standardy szyfrowania symetrycznego:</p> <p>Algorytm : Długość klucza</p> <p>AES : 128 bitów i wzwyż</p> <p>Twofish : 256 bitów i wzwyż</p> <p>IDEA : 128 bitów</p> <p>CHACHA20 : 256 bitów i więcej</p>
Kryptografia	Zalecane tryby to CBC, CFB, OFB, CTR z wykorzystaniem wektora inicjalizującego (IV – Initialization Vector) generowanego za każdym razem.
Kryptografia	<p>Dopuszczalne są następujące standardy szyfrowania asymetrycznego:</p> <p>Algorytm : Długość klucza</p> <p>RSA : 2048 bitów i wzwyż</p> <p>ECC : 224 bity i wzwyż</p>
Kryptografia	<p>Dopuszczalne są następujące standardy wyliczania skrótów:</p> <p>Algorytm :</p> <p>SHA-2</p> <p>SHA-3</p> <p>RIPEMD-160</p>



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 wzwyż ECDSA : 224 bity i wzwyż DSA : 2048 bitów i wzwyż
Kryptografia	Klucze kryptograficzne służące do zabezpieczenia danych POWINNY być generowane lokalnie w infrastrukturze HSM Zamawiającego.
Aplikacje webowe	Tworzone aplikacje webowe MUSZĄ być wolne od podatności i błędów identyfikowanych jako 10 najczęstszych według aktualnej listy OWASP TOP 10.
Aplikacje webowe	<p>Niezależnie od aktualnej zawartości listy OWASP TOP 10 aplikacje webowe MUSZĄ być wolne od następujących podatności i błędów:</p> <ul style="list-style-type: none"> <li>a) Injection - możliwości wstrzykiwania nieautoryzowanych komend w przekazywanych parametrach do aplikacji,</li> <li>b) Broken Authentication and Session Management - możliwości przechwytywania haseł oraz identyfikatorów sesji, zarówno podczas transmisji oraz ich przechowywania,</li> <li>c) Cross Site Scripting (XSS) – możliwości osadzenia kodu w treści atakowanej strony,</li> <li>d) Insecure Direct Object References – możliwości bezpośredniego nieautoryzowanego odwoływania się do obiektów poprzez modyfikację parametrów,</li> <li>e) Security Misconfiguration - błędów w konfiguracji w postaci: <ul style="list-style-type: none"> <li>i. braków w aktualizacji komponentów,</li> <li>ii. niewyłączenia nieużywanych usług, kont, stron, portów,</li> <li>iii. braku zamiany domyślnych haseł,</li> </ul> </li> <li>iv. wyświetlania kodu błędów oraz stosu wywołań w przypadku wystąpienia błędu aplikacji,</li> <li>f) Sensitive Data Exposure – podatności w przetwarzaniu danych wrażliwych w postaci: <ul style="list-style-type: none"> <li>i. przesyłania danych w postaci jawnej,</li> <li>ii. przechowywania danych w postaci jawnej,</li> <li>iii. używania słabych algorytmów kryptograficznych,</li> </ul> </li> <li>v. słabych – krótkich – kluczy kryptograficznych,</li> <li>v. nieodpowiedniego zarządzania kluczami kryptograficznymi,</li> <li>g) Missing Function Level Access Control – błędów w aplikacji w postaci: <ul style="list-style-type: none"> <li>i. braku ograniczenia dostępu w przypadku nieuwierzytelniania,</li> <li>ii. braku ograniczenia dostępu do zasobów zawierających dane konfiguracyjne, logi zdarzeń, pliki źródłowe,</li> <li>iii. braku ograniczenia dostępu do zasobów w zależności od uprawnień,</li> </ul> </li> <li>h) Cross-Site Request Forgery (CSRF) – możliwości przesyłania natychmiastowych żądań do aplikacji,</li> <li>i) Using Components with Known Vulnerabilities – używania komponentów, modułów i bibliotek ze znanymi podatnościami,</li> <li>j) Unvalidated Redirects and Forwards – braku walidacji parametrów zawierających adresy przekierowania i przeniesienia.</li> </ul>
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	<p>Aplikacja webowa MUSI zapewniać mechanizmy zapewniające kontrolę sesji uwierzytelnionego Użytkownika poprzez stosowanie unikalnego identyfikatora. Względem Identyfikatora sesji są następujące wymagania:</p> <ul style="list-style-type: none"> <li>a) NIE MOŻE być krótszy niż 128 bitów,</li> <li>b) MUSI być losowy,</li> <li>c) MUSI być generowany z jak najszerszego zestawu znaków,</li> <li>d) MUSI być unikatowy dla Użytkowników danej aplikacji,</li> <li>e) MUSI być zmieniany/generowany przy uwierzytelnieniu Użytkownika,</li> <li>f) MUSI być zmieniany/deaktywowany przy wylogowaniu Użytkownika</li> <li>g) MUSI być zmieniany/generowany przy przejściu pomiędzy HTTP i HTTPS,</li> <li>h) POWINIEN być akceptowany za poprawny tylko ten identyfikator, który został wygenerowany przez aplikację,</li> <li>i) MUSI być unieważniany po określonym czasie bezczynności Użytkownika,</li> <li>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,</li> <li>k) NIE MOŻE być ujawniany w komunikatach błędów i logach,</li> <li>l) MUSI być unieważniany i zmieniany lub usuwany przy wylogowaniu Użytkownika,</li> <li>m) NIE MOŻE być zapamiętywany w przeglądarce (brak funkcji zapamiętaj mnie),</li> <li>n) Cookie zawierające uwierzytelnione identyfikatory sesji MUSZĄ mieć ustawione atrybuty domain i path odpowiednio dla lokalizacji.</li> </ul>
Aplikacje webowe	<p>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.</p>
Aplikacje webowe	<p>Dla Cookie sesyjnych MUSZĄ być ustawione opcje Secure oraz HttpOnly.</p>
Aplikacje webowe	<p>Dane uwierzytelniające NIE MOGĄ być przekazywane w parametrach adresu URL.</p>
Aplikacje webowe	<p>Aplikacja MUSI posiadać mechanizm ochrony przed 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.</p>
Aplikacje webowe	<p>Pola służące do wprowadzania Hasła MUSZĄ mieć wyłączoną funkcję automatycznego uzupełnienia i zapamiętywania.</p>
Aplikacje webowe	<p>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'.</p>
Aplikacje webowe	<p>Udostępniane przez aplikację strony MUSZĄ mieć zdefiniowany nagłówek X-XSS-Protection. Nagłówek MUSI mieć następującą postać: X-XSS-Protection: 1; mode=block;</p> <ul style="list-style-type: none"> <li>a) wartość 1 pozwala na filtrowanie ze względu na XSS,</li> <li>b) wartość mode=block pozwala na blokowanie przez przeglądarkę wykonanie kodu w przypadku wykrycia podejrzanego skryptu.</li> </ul>

Aplikacje webowe	<p>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</p> <p>a) wartość max-age=31536000 wymusza, że wszelkie zapytania w przyszłości określonej przez max-age do danej witryny muszą odbywać się po HTTPS,</p> <p>b) wartość includeSubDomains wymusza, że wszystkie odwołania na stronie i poddomenach zamieniane są na odwołania po HTTPS.</p>
Aplikacje webowe	Aplikacja POWINNA dla zapytań HTTP dopuszczać jedynie metody GET oraz POST.
Aplikacje webowe	Wysyłane pliki od Użytkownika do aplikacji POWINNY być sprawdzane pod względem zawartości złośliwego kodu.
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.
Zarządzanie Bezpieczeństwem	MUSI być zapewniony udokumentowany model bezpieczeństwa Systemu zgodnie z załącznikiem nr 3 do PROC 55036
Zarządzanie Bezpieczeństwem	MUSZĄ być zapewnione zdefiniowane i opisane funkcje zarządzania bezpieczeństwem Systemu
Zarządzanie Bezpieczeństwem	MUSI być zapewniona pełna identyfikowalność zmian parametrów i reguł Systemu
Zarządzanie Bezpieczeństwem	MUSI być zapewniona możliwość tworzenia kont użytkowników o różnych zakresach uprawnień
Zarządzanie Bezpieczeństwem	MUSI być zapewniona możliwość ograniczenia dostępu użytkownika do określonych danych (w zależności od funkcji)
Zarządzanie Bezpieczeństwem	MUSI być zapewnione zintegrowane zarządzanie bezpieczeństwem, które pozwoli administratorom na tworzenie/mapowanie użytkowników i przyznawanie im uprawnień do określonych operacji na określonych danych w oparciu o role i grupy.
Zarządzanie Bezpieczeństwem	MUSI być zapewniona możliwość automatycznego wylogowania użytkownika z Systemu w przypadku braku aktywności w sesji (brak aktywności w określonym i konfigurowalnym przez administratora przedziale czasu) i uwolnienie wszystkich zajmowanych zasobów, zapewniając integralność danych. Użytkownik MUSI zostać poinformowany wcześniej o tym fakcie stosownym komunikatem na ekranie.
Zarządzanie Bezpieczeństwem	MUSI być zapewniona dokumentacja opisująca zasady bezpiecznego użytkowania Systemu z punktu widzenia użytkownika oraz administratora
Zarządzanie Bezpieczeństwem	<p>System MUSI gwarantować pełną kontrolę administracyjną minimum w zakresie:</p> <p>a) rejestracji zmian konfiguracji</p> <p>b) rejestracji dokonywania poprawek</p> <p>c) rejestracji uaktualnień Systemu.</p>
Zarządzanie Bezpieczeństwem	System Back-office będzie zintegrowany z korporacyjną domeną Active Directory i w tym zakresie MUSI spełniać Polityki Bezpieczeństwa

Zarządzanie Bezpieczeństwem	MUSI zostać zapewniona możliwość konfiguracji z poziomu administracyjnego różnorodnych mechanizmów uwierzytelniania (SSO, bez SSO, dodatkowe stopnie uwierzytelnienia np. SMS) w oparciu o przynależność do odpowiednich grup.
Ochrona Danych	MUSI być zapewniona Poufność (przechowywanych i przesyłanych) wrażliwych danych we wszystkich komponentach Systemu (np. w aplikacji mobilnej).
Ochrona Danych	MUSI być zapewniona Integralność danych podczas przetwarzania i przechowywania przez System
Ochrona Danych	MUSI być zapewniona ochrona wszystkich danych przed ich nieautoryzowanym usunięciem
Ochrona Danych	Dane uwierzytelniające MUSZĄ być składowane w postaci zaszyfrowanej, uniemożliwiającej ich nieautoryzowane odczytanie i zdekodowanie.
Uprawnienia Dostępu Do Systemu	POWINNA być zapewniona funkcjonalność wsparcia dla uwierzytelniania wieloczynnikowego.
Uprawnienia Dostępu Do Systemu	MUSI być zapewniona dodatkowa autoryzacja osób uprawnionych do konfigurowania i modyfikowania istotnych parametrów Systemu
Uprawnienia Dostępu Do Systemu	MUSI być zapewniony limitowany dostęp do informacji audytowych i udokumentowany sposób kontrolowania zakresu dostępu.
Uprawnienia Dostępu Do Systemu	Administratorzy Systemu MUSZĄ mieć niezależne profile autoryzacji.
Uprawnienia Dostępu Do Systemu	Struktura profili autoryzacji MUSI wspierać możliwość konfigurowania i rozbudowy przez administratorów.
Uprawnienia Dostępu Do Systemu	System MUSI rejestrować i przechowywać wszelkie zmiany profili autoryzacji lub przydziału profili użytkownikom w sposób, który zapewni możliwość zweryfikowania jakimi uprawnieniami dysponował dany użytkownik w dowolnym momencie jego historii pracy z Systemem.
Uprawnienia Dostępu Do Systemu	Profile autoryzacyjne MUSZĄ pozwalać na szczegółowe przydzielanie uprawnień użytkownikom w oparciu o grupy i role, a w szczególności muszą wskazywać: a) uprawnienia do komponentów Systemu b) uprawnienia do poszczególnych funkcji Systemu c) uprawnienia do poszczególnych raportów Systemu d) uprawnienia do poszczególnych obszarów danych Systemu e) uprawnienia do określonych logicznych fragmentów obszarów danych (np. konkretnych kategorii kontrahentów czy konkretnych kodów MPK). Poprzez „uprawnienia” należy rozumieć w szczególności: brak dostępu, pełny dostęp, dostęp tylko do odczytu, możliwość eksportu.
Uprawnienia Dostępu Do Systemu	System MUSI mieć możliwość nadawania uprawnień do transakcji/funkcjonalności Systemu oraz do danych i wynikowe uprawnienia MUSZĄ być logicznym iloczynem uprawnień do danych i funkcji.
Uprawnienia Dostępu Do Systemu	System MUSI mieć możliwość grupowania uprawnień i przypisywania użytkowników do grupy.
Uprawnienia Dostępu Do Systemu	System MUSI mieć możliwość przeprowadzenia przekrojowych analiz uprawnień użytkowników lub grup użytkowników.
Uprawnienia Dostępu Do Systemu	Dla funkcjonalności udostępnianych w sieci internet, dla których włączona została funkcjonalność samodzielnej rejestracji System MUSI mieć możliwość konfiguracji stosownych zabezpieczeń (np. Captcha, potwierdzenie adresu e-mail).
Uprawnienia Dostępu Do Systemu	System MUSI mieć możliwość autoryzacji numeru, z którego następuje połączenie; połączenia typu call-back. (jeżeli taka funkcjonalność będzie implementowana).

Uprawnienia Dostępu Do Systemu	System MUSI mieć możliwość rejestrowania prób użycia niedozwolonych dla danego użytkownika funkcji Systemu.
Uprawnienia Dostępu Do Systemu	System MUSI zapewniać możliwość blokowania uwierzytelnienia nowych sesji do Systemu (czas i ilość prób konfigurowalna przez administratora) po nieudanych próbach logowania (błędne podanie identyfikatora i/lub hasła). W przypadku błędnego podawania jedynie hasła nie może być blokowane konto użytkownika a jedynie możliwość uwierzytelnienia się w Systemie (szczególnie ważne przy używaniu SSO)
Uprawnienia Dostępu Do Systemu	Dla użytkowników Systemu niepowiązanych z domeną centralną System MUSI zapewnić odpowiednie zabezpieczenie dostępu: a) za pomocą indywidualnych identyfikatorów i haseł dostępu b) poprzez wymaganie minimalnej długości hasła nie krótszej niż 12 znaków (w tym cyfry i znaki specjalne) c) za pomocą wymuszenia okresowej zmiany haseł – kontrola powtórzeń d) za pomocą nieczytelnego wyświetlania hasła na ekranie e) zabezpieczenie Captcha po trzeciej nieudanej próbie logowania f) opcjonalnie w uzgodnieniu z Zamawiającym dodatkowy stopień uwierzytelnienia (np. jednokrotne hasło dostarczone poprzez SMS, certyfikat cyfrowy, autentykator generujący jednokrotne hasło, karta mikroprocesorowa, profil zaufany).
Uprawnienia Dostępu Do Systemu	System POWINIEN wspierać możliwość wykorzystania kwalifikowanego i niekwalifikowanego podpisu elektronicznego do autoryzowania dowolnych transakcji w Systemie.
Uprawnienia Dostępu Do Systemu	Każda próba połączenia, zarówno dla modułów interaktywnych, jak i nieinteraktywnych MUSI podlegać procesowi uwierzytelnienia i autoryzacji.
Uprawnienia Dostępu Do Systemu	Każdy użytkownik Systemu lub inny komponent (moduł funkcjonalny systemu) MUSI posługiwać się unikalnym identyfikatorem z przydzielonymi do niego uprawnieniami. Nie jest możliwa zmiana identyfikatora, a po jego wyrejestrowaniu (dezaktywacji) nie jest możliwe przydzielenie go innej osobie.
Uprawnienia Dostępu Do Systemu	W odniesieniu do kont użytkowników zarządzanych w Systemie MUSI on umożliwiać okresowe (konfigurowalne przez administratora) wymuszanie zmiany haseł oraz definiowanie wymagań na długość, powtarzalność, budowę i wymagalność zmiany hasła przez użytkowników.
Uprawnienia Dostępu Do Systemu	System MUSI posiadać opracowaną ścieżkę autoryzacyjną (np. kod abonencki) przy autoryzacji osoby dzwoniącej do Call Center z zastrzeżeniem, że musi być weryfikowana za każdym razem tylko losowa część (aby ewentualne podsłuchanie rozmowy nie pozwoliło wykorzystać przechwyconych informacji) - jeżeli taka funkcjonalność będzie implementowana.
Uprawnienia Dostępu Do Systemu	Procedura ustawiania hasła dla klientów Spółki w przypadku jego utraty MUSI być udokumentowana i zapewniać odporność na możliwość nieautoryzowanego nadużycia lub użycia po zdefiniowanym czasie. Powinna uwzględniać możliwość wykorzystania dodatkowych mechanizmów uwierzytelniania jeżeli będą stosowane.
Audyt I Raportowanie	System MUSI zapewnić miejsce do przechowywania informacji na temat audytu / logów (np. tabele logów, pliki logów).
Audyt I Raportowanie	MUSI być zapewnione wsparcie dla audytu operacji (tworzenia, przeglądania, aktualizacji, usuwania).
Audyt I Raportowanie	MUSI być zapewnione wsparcie dla logowania / audytowania informacji dotyczącej logowania, wylogowania i zdarzeń aplikacji.
Audyt I Raportowanie	MUSI być zapewniona możliwość czasowego ustawienia śledzenia w Systemie wszystkich aktywności użytkowników i administratorów.
Audyt I Raportowanie	MUSI być zapewnione posiadanie przez każdą transakcję / operację indywidualnego identyfikatora / numeru referencyjnego specyficznego dla Systemu, umożliwiającego identyfikację ciągu zdarzeń w Systemie w celach rekonylacji i audytu.

Audyt I Raportowanie	MUSI być zapewniony dostęp do raportów o logowaniach i działaniach użytkowników.
Audyt I Raportowanie	MUSI być zapewniony dostęp do raportów o wszelkich nieudanych próbach logowania.
Audyt I Raportowanie	MUSI być zapewniony dostęp do rejestrów zawierających opis błędów, które wystąpiły w systemie (stack trace).
Audyt I Raportowanie	Rozwiązanie MUSI zapewnić mechanizmy weryfikacji integralności danych, plików konfiguracyjnych i krytycznych obszarów Systemu
Audyt I Raportowanie	System MUSI zapewniać mechanizmy audytowe, rejestrujące zdarzenia użytkowników Systemu (w tym kont serwisowych) i administratorów w dzienniku transakcji w zakresie opisanym w sekcji "Audyt Działań i Operacji w Systemie" oraz dodatkowo: a) konfigurowalna wielkość dziennika transakcji z możliwością automatycznej archiwizacji b) reglamentowany dostęp do dziennika dla wybranych grup osób
Audyt I Raportowanie	Interfejsy interaktywne (GUI) MUSZĄ zapisywać w logu audytowym każdą operację użytkownika oraz administratora po włączeniu tej funkcjonalności na określony czas.
Audyt I Raportowanie	Wymagany jest interfejs GUI do przeglądania i analizy zapisów w logu audytowym.
Audyt I Raportowanie	Wymagana jest możliwość eksportowania zapisów z logów audytowych do plików o ustalonej strukturze (pliki płaskie, csv, xml).
Audyt I Raportowanie	Poziom szczegółowości zapisu do logów audytowych MUSI być konfigurowalny lecz nie mniejszy niż zapisano to we wcześniejszym wymaganiu w sekcji "Audyt Działań i Operacji w Systemie"
Audyt I Raportowanie	System MUSI posiadać narzędzia do oceny zdarzeń systemowych i przypisywania im wag i priorytetów. Na ich bazie będą definiowane alerty kierowane do osób zarządzających odpowiednimi obszarami Systemu.
Audyt I Raportowanie	System MUSI posiadać narzędzie do definiowania logów zdarzeń systemowych wg zestawu określonych kryteriów.
Audyt I Raportowanie	Każda operacja wykonana w Systemie MUSI być przypisana do konkretnego identyfikatora użytkownika.
Audyt I Raportowanie	Zmiany istotnych danych w Systemie (zakres uzgodniony z Zamawiającym) MUSZĄ być rejestrowane odrębnie w sposób pozwalający na określenie kto, kiedy i jakie dane zmienił wraz z informacją o poprzedniej ich zawartości.
Audyt I Raportowanie	System MUSI zapewniać możliwość generowania raportów odnośnie przetwarzanych danych osobowych (konkretnej osoby) minimum w zakresie: a) uzyskania informacji jakie szczegółowe dane osobowe są zebrane w Systemie b) uzyskania informacji od kiedy są przetwarzane dane (włączając informacje o zgodzie użytkownika) c) uzyskania informacji o źródle, z którego pochodzą dane (użytkownik Systemu lub system zewnętrzny) d) uzyskania informacji do jakich zewnętrznych systemów dane są udostępniane/przekazywane
Audyt I Raportowanie	Zapewnione MUSI być wsparcie Wykonawcy Systemu w przeprowadzeniu przez Zamawiającego (zewnętrznego lub wewnętrznego) audytu bezpieczeństwa rozwiązania (w tym testów penetracyjnych wykrywających podatności Systemu) przed produkcyjnym uruchomieniem
Komunikacja	Zapewniona MUSI być możliwość integracji Systemu z zewnętrznymi systemami typu SIEM poprzez definiowanie eksportu logów na każdym poziomie (systemowe, aplikacyjne, audytowe itp.) do wskazanych serwerów i z parametrami komunikacyjnymi konfigurowalnymi przez administratora
Komunikacja	Logi eksportowane przez moduły tworzone specjalnie na potrzeby Systemu POWINNY mieć jedno ze standardowych, dobrze udokumentowanych formatów (preferowany syslog - RFC 5424) tak aby możliwa była integracja z zewnętrznymi systemami typu SIEM



Komunikacja	Strefa DMZ MUSI być zabezpieczona zaporami sieciowymi (firewall) zarówno od strony Systemu jak i od strony innych sieci. Reguły na zaporach MUSZĄ pozwalać jedynie na konkretne połączenia do DMZ z sieci wewnętrznej Systemu oraz z innych sieci. Zapory sieciowe MUSZĄ analizować ruch zarówno na poziomie reguł sieciowych oraz na poziomie aplikacyjnym (analiza zawartości pakietów), zezwalać jedynie na określone protokoły oraz powinny kontrolować zgodność przesyłanych danych z tymi protokołami
Komunikacja	Dozwolony jest jedynie ruch inicjowany z sieci wewnętrznej Systemu w kierunku strefy DMZ a zabroniony jest jakikolwiek ruch sieciowy inicjowany w kierunku odwrotnym
Komunikacja	Serwery w strefie DMZ POWINNY zawierać jedynie wybrane dane z systemów wewnętrznych i jeśli to możliwe funkcjonalnie dane te POWINNY być jedynie do odczytu
Komunikacja	System MUSI zapewniać wsparcie dla silnego uwierzytelniania wieloskładnikowego z wykorzystaniem centralnego PKI w GK PGE. Dostęp zdalny do zasobów wewnętrznych MUSI być realizowany dodatkowo poprzez systemy VPN
Komunikacja	System MUSI integrować się z korporacyjnym katalogiem LDAP w sposób zapewniający Poufność
Komunikacja	Wymiana danych pomiędzy poszczególnymi elementami Systemu MOŻE odbywać się z użyciem nieszyfrowanego protokołu (opartego o protokół TCP/IP) tylko w ramach strefy bezpiecznej z wyłączeniem informacji o danych uwierzytelniających
Komunikacja	MUSI być zapewniona segmentacja (separacja fizyczna lub logiczna VLAN/VxLAN) pomiędzy komponentami architektury Systemu i środowiskami np. PROD/TEST
Komunikacja	Zapewniona jest separacja dostępów (wykorzystanie różnych komponentów warstwy prezentacji/serwerów WWW) dla użytkowników wewnętrznych oraz zewnętrznych, łączących się z internetu
Komunikacja	Warstwa komunikacji Systemu z systemami OT MUSI być zgodna z Polityką Bezpieczeństwa Systemów OT (do uzgodnienia na etapie realizacji).
Komunikacja	Komunikacja Systemu do i z systemami OT MUSI wykorzystywać warstwę pośredniczącą (DMZ OT, ReverseProxy, dedykowane szyny komunikacyjne)
Komunikacja	MUSI być zapewnione wsparcie Wykonawcy Systemu w procesie testowania i dopuszczania nowych wersji aplikacji webowej zabezpieczonej firewallem aplikacyjnym (Web Application Firewall)
Komunikacja	Sesja dostępu zdalnego Wykonawcy do komponentu Systemu w trybie administracyjnym będzie rejestrowana w dedykowanym komponencie bezpieczeństwa.
Komunikacja	Dostęp do środowiska produkcyjnego Systemu dla pracowników Wykonawcy będzie domyślnie ograniczony. Każdorazowo dostęp dla pracowników Wykonawcy wymagać będzie zgody upoważnionego przedstawiciela Zamawiającego. Zgoda ta ma charakter czasowy i MOŻE być udzielona maksymalnie na okres 5 dni roboczych.
Backup I Archiwizacja	MUSZĄ być zapewnione zintegrowane mechanizmy wykonywania i przywracania kopii zapasowych wszystkich tabel, plików i innych informacji (np. konfiguracji).
Backup I Archiwizacja	MUSI być zapewniona możliwość wykonywania automatycznej archiwizacji danych w oparciu o zdefiniowane kryteria takie jak zakres danych, interwał wykonywania archiwizacji czy objętość danych po przekroczeniu której ma zostać wykonana archiwizacja.
Backup I Archiwizacja	MUSI być zapewniony zintegrowany dostęp do zarchiwizowanych danych Systemu.
Backup I Archiwizacja	System MUSI umożliwiać realizowanie kopii danych Systemu w technologii „on-line” z wykorzystaniem automatycznych narzędzi do jej planowania i przeprowadzania.



Backup i Archiwizacja	System MUSI umożliwiać odtwarzanie kopii danych do punktu w czasie + dane z logów transakcyjnych.
Dostępność Systemu	MUSI być zapewnione narzędzie do ciągłego monitorowania pracy systemu i automatycznego powiadamiania administratorów systemu w przypadku wystąpienia problemów.
Dostępność Systemu	Wszystkie elementy Systemu MUSZĄ być zaprojektowane w celu zapewnienia wysokiej dostępności na poziomie sprzętowym i aplikacyjnym. Rozwiązanie MUSI być pozbawione pojedynczego punktu awarii (No Single Point of Failure).
Dostępność Systemu	MUSZĄ być zapewnione odpowiednie procedury bezpiecznej aktualizacji oprogramowania, korekt błędów i innych modyfikacji Systemu.
Dostępność Systemu	System MUSI posiadać wewnętrzne mechanizmy wykrywania błędów funkcjonowania Systemu i ich rejestrację w dzienniku.
Dostępność Systemu	System MUSI wykonywać funkcję automatycznego powiadamiania administratora (w formie komunikatów) o wystąpieniu błędu bezpośrednio na konsolę administracyjną (log błędów na ekranie).
Dostępność Systemu	System MUSI wykonywać funkcję automatycznego powiadamiania administratora (w formie komunikatów) o wystąpieniu błędu poprzez e-mail.
Dostępność Systemu	System MUSI gwarantować możliwość wykonywania kopii rezerwowych bez potrzeby wstrzymania pracy w Systemie.
Dostępność Systemu	Rozwiązanie MUSI posiadać udokumentowane i przetestowane procedury przywracania Systemu po awarii dowolnego komponentu Systemu.
Dostępność Systemu	System MUSI posiadać narzędzia do monitorowania ogólnej wydajności Systemu. Raporty z tego narzędzia będą dostępne dla administratorów Systemu.
Dostępność Systemu	Dla Systemu MUSZĄ być uzgodnione pomiędzy Wykonawcą i Zamawiającym poziom RPO i czas RTO dla uzgodnionego minimalnego poziomu działania usług biznesowych MBCO
Wytwarzanie oprogramowania	Oferent w każdym aspekcie dostępu do danych/informacji MUSI dokładać wszelkich najlepszych starań, aby zapewnić ich: poufność, integralność, dostępność oraz rozliczalność. Zarówno w obszarach przechowywania danych, jak i podczas ich transportu pomiędzy komponentami „Systemu” lub integracji z innymi „Systemami”. Należyta dokładność POWINNA być stosowana już na etapie analizy, jak i w trakcie projektowania oraz realizacji rozwiązań.
Wytwarzanie oprogramowania	Proces wytwarzania Systemu MUSI być zgodny z Normami ISO/IEC 27001 Zarządzanie Bezpieczeństwem Informacji (np. zapewnienie poufności kodu źródłowego).
Wytwarzanie oprogramowania	Proces wytwarzania Systemu MUSI stosować zalecenia fundacji OWASP „Open Web Application Security Project” oraz wykorzystywać wstępne testowanie wg aktualnych zaleceń ASVS "Application Security Verification Standard".
Wytwarzanie oprogramowania	Proces wytwarzania Systemu MUSI stosować najlepsze praktyki programistyczne w zakresie bezpieczeństwa (analiza kodu, weryfikacja stosowanych bibliotek itp.).
Wytwarzanie oprogramowania	Proces wytwarzania Systemu POWINIEN wykorzystywać preferowane nowoczesne metody autentykacji z pominięciem hasła tzw. „password-less”.
Zgodność z normami	Wymagana jest zgodność z normą ISO/IEC 27001 Zarządzanie Bezpieczeństwem Informacji
Zgodność z normami	Wymagana jest zgodność z normą ISO 22301 Zarządzanie Ciągłością Działania
Najlepsze praktyki i niezależne certyfikacje	POWINNY być stosowane zalecenia / benchmarks CIS (ang. Center for Internet Security) w zakresie wykorzystania zaleceń kontrolnych i utwardzania Systemu.

Kontrola łańcucha dostaw	Dostawca zapewnia współpracę z Zamawiającym i współuczestniczenie w przeprowadzanych audytach i ankietach potwierdzenia zgodności z normami oraz spełnieniem wymagań kontroli RODO oraz uKSC w ramach dostarczanych komponentów Systemu
Kontrola łańcucha dostaw	Aktualizacje i nowe wersje subkomponentów Systemu MUSZĄ zostać poddane weryfikacji na obecność malware i nieautoryzowanej modyfikacji przed instalacją w komponentach docelowych Zamawiającego
Kontrola łańcucha dostaw	Zapewnienie ze strony Dostawcy należytej staranności w wypełnieniu najlepszych praktyk bezpieczeństwa MUSI być realizowane nie tylko w warstwie technologicznej ale przede wszystkim organizacyjnej oraz potwierdzone w umowach serwisowych.