

WYMAGANIA BEZPIECZEŃSTWA DLA SYSTEMÓW TELEINFORMATYCZNYCH

Skróty użyte na potrzeby niniejszego dokumentu:

API	- Application Programming Interface (ang.) – interfejs programistyczny aplikacji pozwalający na komunikację z aplikacją
CRL	- Certificate Revocation List (ang.) - lista unieważnionych certyfikatów
CPD	- Centrum Przetwarzania Danych (ang. Data center) – infrastruktura budowlana i środowiskowa zapewniająca wymagane poziomy dostępności i ciągłość usług
DMZ zaufania	- Demilitarized zone (ang.) – strefa zdemilitaryzowana lub ograniczonego zaufania
HTTP	- Hypertext Transfer Protocol (ang.) – protokół w warstwie aplikacyjnej służący do wymiany informacji pomiędzy rozproszonymi systemami informacyjnymi, używany do obsługi stron WWW
HSTS	- HTTP Strict Transport Security (ang.) - mechanizm zabezpieczenia serwowanych stron polegający na blokowaniu zmian w parametrach protokołu
HTML	- HyperText Markup Language (ang.) – język znaczników wykorzystywany do tworzenia stron WWW
HTTPS	- Hypertext Transfer Protocol Secure (ang.) – zabezpieczony HTTP poprzez zastosowanie SSL/TLS
IAM	- Identity and Access Management (ang.) – zarządzanie tożsamością i dostępem
IoT	- Internet of Things (ang.) – Internet rzeczy, internet przedmiotów
PGE, PGE S.A.	- PGE Polska Grupa Energetyczna S.A.
PIM	- Privileged Identity Management (ang.) – zarządzanie dostępem do Kont Technicznych
OWASP	- Open Web Application Security Project (ang.) – międzynarodowa organizacja, której celem są działania na rzecz poprawy bezpieczeństwa oprogramowania
OWASP TOP 10	- dziesięć najczęstszych podatności i błędów występujących w wytwarzanym oprogramowaniu według organizacji OWASP
RODO	- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
SIEM	- Security Information and Event Management (ang.) – zarządzanie informacjami i zdarzeniami bezpieczeństwa
SSL	- Secure Socket Layer (ang.) – protokół w warstwie transportowej/sesyjnej zapewniający poufność, integralność oraz uwierzytelnienie serwera

SSO	- Single Sign-on (ang.) - możliwość jednorazowego zalogowania się do usługi sieciowej i uzyskania dostępu do wszystkich autoryzowanych zasobów zgodnych z tą usługą
Spółka, Spółki	- podmiot / podmioty prawa handlowego wchodzące w skład Grupy Kapitałowej PGE
TLS	- Transport Layer Security (ang.) - protokół w warstwie transportowej/sesyjnej zapewniający poufność, integralność oraz uwierzytelnienie serwera
URI	- Uniform Resource Identifier (ang.) – ujednolicony identyfikator jednoznacznie wskazujący na zasób
XSS strony	- Cross Site Scripting – możliwości osadzenia kodu w treści atakowanej strony
RPO	- 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
RTO	- 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
MBCO	- Minimum Business Continuity Objective - minimalny poziom odtworzenia usługi teleinformatycznej, który jest akceptowalny dla Spółki do osiągnięcia jej celów biznesowych w sytuacji krytycznej

Definicje pojęć użyte na potrzeby niniejszego dokumentu:

Administrator Systemu Teleinformatycznego (Administrator) - 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.

Bezpieczeństwo Informacji -zapewnienie Poufności, Integralności i Dostępności przetwarzanych informacji czyli zabezpieczanie jej przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem.

Dostępność - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.

Dziennik Systemu Teleinformatycznego / Dziennik – 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.

Grupa Kapitałowa PGE (GK lub GK PGE) – PGE oraz Spółki względem których PGE posiada status spółki dominującej w rozumieniu artykułu 4 § 1 punkt 4 kodeksu spółek handlowych.

Hasło - ciąg znaków, który służy do uwierzytelniania w Systemie Teleinformatycznym.

HTTP cookie, Cookie – wysłany przez aplikację webową i przechowywany przez przeglądarkę ciąg znaków, wykorzystywany – przesyłany - w dalszej części komunikacji z przeglądarki do aplikacji webowej.

Identyfikator w Systemie Teleinformatycznym (Identyfikator) - unikalny ciąg znaków jednoznacznie identyfikujący w Systemie Teleinformatycznym Użytkownika lub inny System Teleinformatyczny.

Integralność - właściwość zapewnienia dokładności i kompletności. Integralność informacji/danych - oznacza, że dane nie będą w nieautoryzowany lub przypadkowy sposób zmodyfikowane przez nieuprawnione osoby.

Konto - zbiór praw dostępu do Systemu Teleinformatycznego, dedykowany dla Użytkownika lub innego Systemu Teleinformatycznego identyfikowanych przez Identyfikator i Środki Uwierzytelniania

Konto Techniczne – Konto z którego korzysta więcej niż jeden Użytkownik i/lub System, nie przynależące do określonego Użytkownika.

Konto Techniczne Interaktywne – 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.

Konto Techniczne Nieinteraktywne – Konto Techniczne, którego uprawnienia umożliwiają wykonywanie określonych czynności administracyjnych w Systemie bez możliwości uzyskania dostępu do konsoli systemowej po zalogowaniu się na to Konto.
Konto Serwisowe – Konto Techniczne, którego uprawnienia umożliwiają wykonywanie określonych czynności w Systemie i używane do cyklicznych czynności serwisowych (np. usługi serwisowe, kopia zapasowa).
Konto Współdzielone – Konto Techniczne Interaktywne nie będące Kontem Serwisowym wykorzystywane między innymi w celach technicznej obsługi Systemu Teleinformatycznego.
Poufność - właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
Przetwarzanie Informacji - jakiekolwiek operacje wykonywane na informacji, w szczególności takie jak ich zbieranie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie, przesyłanie i usuwanie.
Strefa zdemilitaryzowana (DMZ) - jest to wydzielany na zaporze 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).
System Teleinformatyczny (System) - zespół środków technicznych wraz z oprogramowaniem tworzący logiczną i nierozzerwalną całość wyodrębnioną ze względu na dostarczaną funkcjonalność przy założeniu, że głównym jego celem jest Przetwarzanie Informacji.
Środki Uwierzytelniania - hasła, hasła jednorazowe, klucze i certyfikaty cyfrowe, tokeny sprzętowe (karty, klucze, transpondery), sygnatury biometryczne lub ich kombinacje umożliwiające skuteczne uwierzytelnienie Użytkownika w Systemie.
Użytkownik - osoba uprawniona do korzystania z Systemu Teleinformatycznego.

1.1 POSTANOWIENIA OGÓLNE

1.1.1 Następujące słowa kluczowe są używane w dokumencie do określenia zawartego wymagania:

- słowa MUSI, WYMAGANY lub NIE MOŻE, ZABRONIONE oznaczają, że treść zapisu musi być bezwzględnie przestrzegana,
- słowa POWINNO, ZALECANE lub NIE POWINNO, NIEZALECANE oznaczają, że dopuszczalne jest niezastosowanie się do treści zapisu.

1.1.1.2 Departament odpowiedzialny za obszar cyberbezpieczeństwa w PGE Systemy S.A. rekomenduje unikanie zakupu rozwiązań informatycznych pochodzących z krajów prowadzących nieprzychylną lub wrogą politykę wobec Rzeczypospolitej

Polskiej, krajów objętych sankcjami Rady Bezpieczeństwa NZ lub Unii Europejskiej oraz krajów wspierających terroryzm.

1.2 DOKUMENTACJA SYSTEMU TELEINFORMATYCZNEGO

1.2.1 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.

1.2.2 Do dokumentacji Systemu MUSI być dołączona dokumentacja bezpieczeństwa. W dokumentacji bezpieczeństwa MUSZA być zamieszczone informacje na temat konfiguracji i mechanizmów w Systemie realizujących wymagania opisywane poniżej.

1.2.3 Dokumentacja Systemu MUSI zawierać „Model bezpieczeństwa systemu” – opisane zastosowane mechanizmy bezpieczeństwa.

1.2.3.1 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.

1.2.3.2 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

1.3 LOKALIZACJA, ŚRODOWISKO I ARCHITEKTURA

1.3.1 System POWINIEN być fizycznie zlokalizowany w Centrum Przetwarzania Danych lub określonym środowisku chmurowym (ang. Cloud) potwierdzone na zgodność z wymaganiami ISO:

- 1.3.1.1 Normą ISO/IEC 27001 Zarządzanie Bezpieczeństwem Informacji
- 1.3.1.2 Normą ISO 22301 Zarządzanie Ciągłością Działania
- 1.3.1.3 Normą ISO/IEC 27017 Bezpieczeństwo Informacji dla usług w Chmurze
- 1.3.1.4 Normą ISO/IEC 27018 Ochrona Danych Osobowych w Chmurze
- 1.3.2 Infrastruktura CPD/Cloud POWINNA gwarantować świadczenie usługi na zdefiniowanym poziomie SLA oraz być zlokalizowana geograficznie na terytorium Europejskiego Obszaru Gospodarczego.
- 1.3.3 System Krytyczny dla działania Spółki POWINIEN być wolny od pojedynczego punktu awarii („No Single Point of Failure”).
- 1.3.4 System POWINIEN mieć dostępne mechanizmy tworzenia i odtwarzania kopii zapasowej z określonymi czasami trwania operacji.
- 1.3.5 Dla Systemów przetwarzających dane osobowe MUSI być stosowane pełne szyfrowanie mocnymi algorytmami baz danych przechowujących te dane.
- 1.3.6 Dla Systemu MUSZĄ być opracowane procedury przywracania po katastrofie.
- 1.3.7 System POWINIEN posiadać co najmniej dwa środowiska: produkcyjne i testowe. System POWINIEN mieć dodatkowo środowiska preprodukcyjne i rozwojowe.
- 1.3.8 Dla Systemu MUSZĄ zostać zdefiniowane parametry RTO, RPO na okoliczność wystąpienia awarii usługi.
- 1.3.9 Dla Systemu MUSZĄ być opracowane procedury przywracania po katastrofie.
- 1.4 OPROGRAMOWANIE ORAZ KONTROLA STANU I ZMIAN W SYSTEMIE**
- 1.4.1 System MUSI zapewniać mechanizmy umożliwiające aktualizację oprogramowania, w szczególności MUSI pozwalać na naprawę błędów związanych z bezpieczeństwem.
- 1.4.2 System MUSI posiadać mechanizmy Kontroli i rejestracji zmian konfiguracji oraz aktualizacji oprogramowania.
- 1.4.3 Dla Systemu MUSI istnieć aktualna lista (w postaci załącznika do dokumentacji bezpieczeństwa) dostępnych aktualizacji bezpieczeństwa, które nie zostały wdrożone, z podanym uzasadnieniem.
- 1.4.4 System POWINIEN wykorzystywać tylko oprogramowanie w wersji wspieranej przez producenta.
- 1.4.5 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).
- 1.4.6 W Systemie NIE POWINNO być zainstalowane oraz uruchomione oprogramowanie, które nie jest konieczne do jego poprawnego działania.
- 1.4.7 W Systemie POWINNY być wdrożone wszystkie udostępniane przez dostawców oprogramowania krytyczne aktualizacje bezpieczeństwa dla wszystkich składników oprogramowania nie później niż 30 dni od daty ich udostępnienia.
- 1.4.8 W Systemie POWINNY być wdrożone mechanizmy do kontroli jego stanu. System MUSI posiadać mechanizmy automatycznego powiadamiania administratora o wystąpieniu błędu.
- 1.4.9 Wykorzystywane w Systemie oprogramowanie MUSI być autoryzowane, tzn. wolne od wirusów, malware z potwierdzonymi prawami licencyjnymi.
- 1.4.10 W przypadku udostępniania aplikacji mobilnej, MUSI być ona cyfrowo podpisana w celu umożliwienia jej identyfikacji, weryfikacji autentyczności i integralności.
- 1.4.11 Treści wyświetlane na urządzeniach mobilnych powinny być „responsywne”, czyli powinny się dostosowywać automatycznie do wielkości ekranu.

1.5 RUCH SIECIOWY

1.5.1

- 1.5.2 System MUSI udostępniać tylko usługi sieciowe niezbędne do jego działania lub obsługi serwisowo-administracyjnej.
- 1.5.3 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.
- 1.5.4 Dostęp serwisowo-administracyjny może być realizowany ze ściśle określonych adresów, rekomendowane jest wykorzystanie stacji przesiadkowych/zarządzających.
- 1.5.5 Komunikacja Systemu z innymi Systemami lub Użytkownikami POWINNA się odbywać za pomocą serwera pośredniczącego. W szczególności dotyczy to ruchu przychodzącego (Reverse Proxy).
- 1.5.6 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.
- 1.5.7 Wszystkie komponenty Systemu MUSZĄ być w sieci jednoznacznie identyfikowane. Do identyfikacji ZALECANE jest wykorzystanie certyfikatów cyfrowych.
- 1.5.8 Wymagany ruch sieciowy MUSI być opisany.
- 1.5.9 Ruch sieciowy przed przekazaniem do realizacji podlega procesowi kontroli zgodności z architekturą Systemu i akceptacji przez departament bezpieczeństwa w PGE Systemy S.A.

1.6 KOMUNIKACJA

- 1.6.1 Interfejsem używanym do komunikacji Użytkownika z Systemem POWINIEN być interfejs WWW.
- 1.6.2 System do komunikacji z Użytkownikiem lub innym Systemem MUSI stosować połączenie zapewniające Integralność i Poufność przesyłanych danych.
- 1.6.3 System do transmisji danych z zastosowaniem protokołu SSL w tym HTTPS POWINIEN stosować protokół TLS v1.2 (lub wyższej, preferowany TLS v1.3) 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 (lub wyższa), preferowane SHA-256.
- 1.6.4 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 (lub wyższa), preferowana SHA-256
 - f. grupa Diffie-Hellman: minimum Group 15, preferowana 19 lub 24
 - g. tryb negocjacji w fazie I: Main mode, Aggressive mode (zabroniony),
 - h. czas ważności kluczy: 3600 sekund.
- 1.6.5 W Systemie MUSZĄ istnieć mechanizmy zapewniające kontrolę i walidację wprowadzanych danych.
 - 1.6.5.1 W przypadku wprowadzania ciągów znaków kontrola danych dotyczy ich formatu i składni.
 - 1.6.5.2 Wszystkie interfejsy dla danych wejściowych do Systemu MUSZĄ mieć zdefiniowane i zastosowane wzorce pozytywnej walidacji.

- 1.6.5.3 Walidacja danych wejściowych do Systemu zakończona niepowodzeniem MUSI odrzucać lub oczyszczać przyjmowane dane.
- 1.6.5.4 Wszystkie interfejsy dla danych wejściowych MUSZĄ posiadać zdefiniowaną stronę kodową np. UTF-8.
- 1.6.5.5 Walidacja danych wejściowych MUSI się odbywać po stronie serwera.
- 1.6.5.6 Wszystkie walidacje danych wejściowych zakończone niepowodzeniem POWINNY być logowane.
- 1.6.5.7 Usługa udostępniana po protokole http lub https MUSI być dostępna odpowiednio na portach 80 i 443.
- 1.6.5.8 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)
- 1.6.5.9 Wymagane jest, aby usługa udostępniana poprzez https posiadała ważny certyfikat SSL wydany przez zaufany urząd certyfikacji.
- 1.6.5.10 Certyfikat wykorzystywany do uwierzytelnienia usługi musi być automatycznie rozpoznawany jako zaufany w systemach operacyjnych i przeglądarkach wykorzystywanych przez użytkowników.
- 1.6.5.11 W przypadku, gdy usługa udostępnia dane poprzez protokół http powinna ona działać na aktualnych i dopuszczonych przez Zamawiającego wersjach następujących przeglądarek internetowych: MS Edge, Mozilla FireFox ESR, Google Chrome.

1.7 ZARZĄDZANIE UŻYTKOWNIKAMI

- 1.7.1 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, PROC 55036/D. Procedura Wymagania bezpieczeństwa dla systemów teleinformatycznych
 - 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.
- 1.7.2 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. ponowne ustawienie hasła związanego 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.
- 1.7.3 System musi posiadać zdefiniowaną i zaimplementowaną procedurę zarządzania kontami i uprawnieniami użytkowników usługi.
- 1.7.4 W przypadku błędnego pięciokrotnego uwierzytelnienia użytkownika do usługi konto użytkownika MUSI być blokowane na co najmniej 10 minut.
- 1.7.5 Konta użytkowników wykorzystywane w usłudze muszą być imienne, tzn. niewspółdzielone.
- 1.7.6 Usługa musi mieć zdefiniowaną procedurę resetu hasła.
- 1.7.7 Proces rejestracji nowych użytkowników i zakładania kont w Systemie musi uwzględniać mechanizmy do weryfikacji podawanych danych np. e-mail, wykluczenia robotów/automatów oraz wykorzystać potwierdzenie osoby rejestrującej się za pośrednictwem bezpiecznych linków aktywacyjnych generowanych automatycznie i aktywnych przez określony, definiowalny okres czasu

1.8 KONTROLA DOSTĘPU

- 1.8.1 Wszystkie Konta techniczne MUSZĄ być zewidencjonowane w dokumentacji bezpieczeństwa systemu. Wszystkie domyślne Hasła MUSZĄ zostać zmienione, a niewykorzystywane Konta zablokowane.
- 1.8.2 System MUSI umożliwiać zdefiniowanie terminu wygasania ważności Konta Użytkownika.
- 1.8.3 Po przekroczeniu daty wygasania, Konto MUSI być przez system automatycznie blokowane.
- 1.8.4 System NIE POWINIEN umożliwiać usuwania Kont. Jeżeli w systemie jest taka funkcjonalność, POWINNA ona być zablokowana.
- 1.8.5 W Systemie MUSI istnieć funkcjonalność trwałego zablokowania Konta, uniemożliwiająca wykorzystanie Konta (zalogowanie się) nawet w przypadku posiadania prawidłowych danych uwierzytelniających.
- 1.8.6 W Systemie MUSI istnieć 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.
- 1.8.7 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).
- 1.8.8 Lista Kont Technicznych MUSI zawierać informację o przeznaczeniu Konta (Konto Współdzielone lub Konto Serwisowe Interaktywne lub Nieinteraktywne)

1.9 UWIERZYTELNIANIE

- 1.9.1 System MUSI zapewniać mechanizmy do uwierzytelniania Użytkowników oraz innych Systemów.
- 1.9.2 System MUSI zapewniać Integralność i Poufność informacji o Kontach, w szczególności o Hasłach oraz innych danych w oparciu o które następuje uwierzytelnienie.
- 1.9.3 System NIE MOŻE bez uwierzytelnienia udostępniać jakichkolwiek informacji lub funkcjonalności, które powinny być dostępne tylko po poprawnym uwierzytelnieniu.
- 1.9.4 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.

- 1.9.5 ZABRONIONE jest wykorzystywanie mechanizmów uwierzytelniania wymagających przesłania do Systemu Hasła Użytkownika.
- 1.9.6 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.)
- 1.9.7 Mechanizm interaktywnego wprowadzania Hasła lub numeru PIN przy uwierzytelnieniu do Systemu MUSI zapewnić Poufność wprowadzanych danych poprzez nie wyświetlanie ciągu wprowadzanych znaków.
- 1.9.8 System MUSI wymuszać stosowanie przez Użytkowników trudnych Haseł, zgodnie z następującymi wymaganiami:
- Hasło Użytkownika składa się z minimum 12 znaków,
 - Hasło Administratora składa się z minimum 15 znaków,
 - Hasło zawiera przynajmniej 1 małą literę (od a do z),
 - Hasło zawiera przynajmniej 1 dużą literę (od A do Z),
 - Hasło zawiera przynajmniej 1 cyfrę (od 0 do 9),
 - Hasło zawiera przynajmniej 1 znak specjalny: !@#\$%^&*(){}[]\|:~';<>?.,/,
 - Hasło nie może zawierać kolejno dwóch identycznych znaków oraz powtarzających się sekwencji znaków,
 - Hasło nie może zawierać znaków diakrytycznych (np. ą, ę),
 - Hasło nie może być identyczne z nazwą Konta lub jego częścią,
 - Hasło nie może być imieniem, nazwiskiem, datą urodzenia,
 - Hasło wymaga zmiany maksymalnie co 90 dni
 - minimalny okres pomiędzy kolejnymi zmianami Hasła to 2 dni,
 - nowe Hasło musi być inne, niż co najmniej 5 ostatnio wprowadzonych Haseł,
 - Hasło nie może zawierać nazwy Konta,
 - Hasło musi składać się z co najmniej 5 różnych znaków,
 - Hasło musi różnić się od poprzedniego co najmniej 3 znakami,
- lub wykorzystywać silne metody uwierzytelniania i dodatkowe mechanizmy autoryzacji.
- 1.9.9 System POWINIEN posiadać mechanizmy do zmiany hasła przez Użytkowników.
- 1.9.10 System POWINIEN wymuszać na Użytkownikach okresowe zmiany Hasła.
- 1.9.11 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).
- 1.9.12 Po pierwszym udanym uwierzytelnieniu Użytkownika w Systemie, System POWINIEN wymusić zmianę Hasła przed udostępnieniem mu jakiegokolwiek innej funkcjonalności.
- 1.9.13 System MUSI posiadać udokumentowane procedury zmiany haseł dla kont technicznych.
- 1.9.14 System POWINIEN wspierać i udostępniać możliwość wykorzystania mechanizmów jednokrotnego uwierzytelniania SSO (Single Sign On) dla użytkowników wewnętrznych, uwierzytelniających się w korporacyjnej domenie Active Directory.
- 1.9.15 Dla każdego Użytkownika oraz innego Systemu MUSZĄ istnieć w Systemie dedykowane Konta..
- 1.9.16 Hasła w Systemie POWINNY być przechowywane w postaci skrótów (ang. Hash) dla których zastosowano ciąg zaburzający (ang. salt).

- 1.9.17 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.

1.10 AUTORYZACJA

- 1.10.1 System MUSI zapewniać mechanizmy do autoryzacji Użytkowników oraz innych Systemów.
- 1.10.2 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.
- 1.10.3 Konta techniczne wykorzystywane w Systemie MUSZĄ mieć przyznany minimalny niezbędny zakres uprawnień.
- 1.10.4 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.
- 1.10.5 System POWINIEN umożliwiać przydzielanie uprawnień Użytkownikom pośrednio poprzez tworzenie grup Użytkowników i przydzielanie uprawnień grupom.
- 1.10.6 Dostęp do funkcji Systemu POWINIEN być zdefiniowany poprzez role w Systemie.
- 1.10.7 Wszystkie ustalone reguły kontroli dostępu do usług, funkcji, danych i obiektów MUSZĄ być wymuszane po stronie serwera.
- 1.10.8 Mechanizmy kontroli dostępu zaimplementowane w Systemie MUSZĄ utrzymywać aktualny stan uprawnień Użytkowników i w przypadku zmiany, ich egzekwowanie powinno być realizowane w trybie natychmiastowym.
- 1.10.9 Dostęp do Systemu zlokalizowanego poza infrastrukturą GK PGE POWINIEN umożliwiać stosowanie dodatkowego stopnia uwierzytelnienia lub innego mechanizmu zabezpieczeń warunkującego dostęp.

1.11 AUDYT DZIAŁAŃ I OPERACJI W SYSTEMIE

- 1.11.1 System MUSI posiadać mechanizmy do tworzenia i przechowywania audytu/logów (np. tabele logów, pliki logów) dotyczących działania Systemu.
- 1.11.2 Do audytu/logowania System POWINIEN wykorzystywać protokół Syslog.
- 1.11.3 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 kodu zwróconego błędu w przypadku niepowodzenia.
- 1.11.4 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).
- 1.11.5 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 większą 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 kod zwróconego błędu w przypadku niepowodzenia.
- 1.11.6 System MUSI mieć możliwość podłączenia do Systemu SIEM Zamawiającego. 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.
- 1.11.7 Preferowanym protokołem przekazywania zdarzeń do SIEM z systemów jest protokół Syslog.
- 1.11.7.1 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
- 1.12 SYNCHRONIZACJA CZASU**
- 1.12.1 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 MOGĄ wykorzystywać kontrolery domeny jako źródło czasu.
- 1.12.2 Synchronizacja czasu dla wszystkich komponentów Systemu POWINNA odbywać się przy pomocy protokołu Network Time Protocol (NTP) lub Simple Network Time Protocol (SNTP).
- 1.13 ZGODNOŚĆ Z PRZEPISAMI PRAWA**
- 6.1.1 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.)

1.14 KRYPTOGRAFIA

1.14.1 Dopuszczalne są następujące standardy szyfrowania symetrycznego:

Algorytm	Długość klucza
AES	128 bitów i wzwyż
Twofish	256 bitów i wzwyż
IDEA	128 bitów
CHACHA20	256 bitów i więcej

Zalecane tryby to CBC, CFB, OFB, CTR z wykorzystaniem wektora inicjalizującego (IV – Initialization Vector) generowanego za każdym razem.

1.14.2 Dopuszczalne są następujące standardy szyfrowania asymetrycznego:

Algorytm	Długość klucza
RSA	2048 bitów i wzwyż
ECC	224 bity i wzwyż

1.14.3 Dopuszczalne są następujące standardy wyliczania skrótów

Algorytm
SHA-2
SHA-3
RIPEMD-160

1.14.4 Dopuszczalne są następujące standardy MAC (Message Authentication Code):

Algorytm
HMAC
CBC-MAC
CMAC
POLY1305

1.14.5 Dopuszczalne są następujące standardy podpisu cyfrowego:

Algorytm	Długość klucza
RSA	2048 bitów i wzwyż
ECDSA	224 bity i wzwyż
DSA	2048 bitów i wzwyż

1.15 WYMAGANIA SZCZEGÓLNE WZGLĘDEM SYSTEMÓW BĘDĄCYCH APLIKACJAMI WEBOWYMI

- 1.15.1 Tworzone aplikacje webowe POWINNY być wolne od podatności i błędów identyfikowanych jako 10 najczęstszych według aktualnej listy OWASP TOP 10.
- 1.15.2 Niezależnie od aktualnej zawartości listy OWASP TOP 10 aplikacje webowe powinny być wolne od następujących podatności i błędów:
- Injection - możliwości wstrzykiwania nieautoryzowanych komend w przekazywanych parametrach do aplikacji,
 - 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 niewierzytelniania,
 - 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.
- 1.15.3 Wykonanie wrażliwych operacji w aplikacji POWINNO być poprzedzone ponownym uwierzytelnieniem.
- 1.15.4 Wszystkie strony oraz zasoby MUSZĄ wymagać uwierzytelnienia za wyjątkiem tych specjalnie przeznaczonych dla dostępu publicznego.
- 1.15.5 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.
- 1.15.6 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.
- 1.15.7 Dla Cookie sesyjnych MUSZĄ być ustawione opcje Secure oraz HttpOnly. (więcej informacji: <https://sekurak.pl/flaga-cookie-httponly/>)
- 1.15.8 Dane uwierzytelniające NIE MOGĄ przekazywane w parametrach adresu URL.
- 1.15.9 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.
- 1.15.10 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.
- 1.15.11 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'.
- 1.15.12 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.
- 1.15.13 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.
- 1.15.14 Aplikacja POWINNA dla zapytań HTTP dopuszczać jedynie metody GET oraz POST.

- 1.15.15 Wysyłane pliki od Użytkownika do aplikacji POWINNY być sprawdzane pod względem zawartości złośliwego kodu. System MUSI dopuszczać zaimportowanie wyłącznie określone kategorie plików.
 - 1.15.16 Przekazywane do aplikacji parametry dotyczące odwołań do plików muszą podlegać sprawdzaniu w celu uniknięcia ataków manipulujących ścieżką tzw. path traversal.
 - 1.15.17 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.
 - 1.15.18 Aplikacja NIE POWINNA wymagać instalacji w przeglądarce internetowej dodatkowych komponentów typu ActiveX, aplet Java.
 - 1.15.19 Aplikacja NIE POWINNA korzystać z komponentów Adobe Flash, Microsoft Silverlight.
- 1.16 WYMAGANIA SZCZEGÓLNE DLA SYSTEMU ULOKOWANEGO W CHMURZE PUBLICZNEJ W MODELU IaaS/FaaS/PaaS/SaaS NADZOROWANEJ PRZEZ DOSTAWCĘ**
- 1.16.1 Wymagane jest posiadanie certyfikacji potwierdzających zgodność z:
 - (a) Normą ISO/IEC 27001 Zarządzanie Bezpieczeństwem Informacji
 - (b) Normą ISO 22301 Zarządzanie Ciągłością Działania
 - (c) Normą ISO/IEC 27017 Bezpieczeństwo Informacji dla usług w Chmurze
 - (d) Normą ISO/IEC 27018 Ochrona Danych Osobowych w Chmurze
 - 1.16.2 Wymagane jest wykorzystanie przez Dostawcę najlepszych praktyk branżowych:
 - (a) CSA – ang. *Cloud Security Alliance certyfikacja STAR ang. Security Trust Assurance and Risk* (<https://www.bsigroup.com/pl-PL/Certyfikacja-CSA-STAR/>)
 - (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*
 - (e) ISVS – ang. *IoT Security Verification Standard*
 - 1.16.3 Rozwiązanie MUSI być zgodne z RODO a przetwarzanie danych odbywa się w granicach EOG (Europejskiego Obszaru Gospodarczego)
 - 1.16.4 Preferowane są lokalizacje przetwarzania danych na terytorium Polski
 - 1.16.5 Dostawca chmury oraz usług w chmurze w każdym aspekcie dostępu do zasobów MUSI 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.
 - 1.16.6 Rozwiązanie MUSI wspierać sposób uwierzytelnienia przez Azure AD lub ADFS Zamawiającego
 - 1.16.7 Rozwiązanie MUSI umożliwiać skonfigurowanie uwierzytelnienia 2 Factor Authentication (uwierzytelnianie 2 składnikowe)
 - 1.16.8 Wymagane jest dopuszczenie możliwości przeprowadzenia szczegółowego audytu dla usług dostarczanych poza infrastrukturą zamawiającego.
 - 1.16.9 Wymagane jest spełnienie oczekiwanego SLA w szczególności brak pojedynczego punktu awarii oraz odpowiednia odporność na awarie komponentów chmurowych.

- 1.16.10 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.
 - 1.16.11 Klucze kryptograficzne wykorzystywane do zabezpieczenia poufności istotnych danych MUSZĄ być generowane lokalnie w infrastrukturze PGE, ich odwołanie ma uniemożliwić możliwość deszyfracji przechowywanych danych poza infrastrukturą Zamawiającego.
 - 1.16.12 Uzgodnione zdarzenia bezpieczeństwa (logi) od warstwy L3 modelu ISO/OSI POWINNY być przekazywane zespołowi PGE – CERT – integracja z SIEM Zamawiającego
 - 1.16.13 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
 - 1.16.14 Wymagana jest integracja z systemem kopii zapasowych Zamawiającego w celu umożliwienia przechowywania dodatkowych kopii danych w infrastrukturze Zamawiającego
 - 1.16.15 Preferowane jest wykorzystanie uniwersalnej warstwy abstrakcji uniezależniającej 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 and. Infrastructure as a Code
 - 1.16.16 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)
- 1.17. **WYMAGANIA DEDYKOWANE DO REALIZACJI PRZEZ DOSTAWCĘ NA ETAPIE WDROŻENIA**
- 1.17.1. Opracowanie przedwdrożeniowej dokumentacji technicznej Systemu w konsultacji z Architektem bezpieczeństwa oraz Cyberbezpieczeństwa Zamawiającego
 - 1.17.2. Uruchomienie uwierzytelniania dwuskładnikowego (2FA) do usług chmurowych (back office) z udziałem kont zakładanych w infrastrukturze AD Zamawiającego i stosowanymi mechanizmami jednokrotnego logowania S-SSO (Seamless SSO) PRT do Azure AD lub ADFS
 - 1.17.3. Wykorzystanie w procesie nadawania uprawnień systemu IAM Zamawiającego
 - 1.17.4. Monitorowanie usług Systemu aby incydenty bezpieczeństwa były obsługiwane przez zespół PGE-CERT (integracja zdarzeń po stronie chmury z systemami Zamawiającego SIEM/SOAR)
 - 1.17.5. Zapewnienie odrębnej kopii zapasowej danych Systemu w infrastrukturze Zamawiającego
 - 1.17.6. 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.

- 1.17.7. Przekazanie niezbędnych kompetencji (szkoleń) zespołowi PGE-CERT w kontekście analizy i reagowania na incydenty bezpieczeństwa w zakresie Systemu po stronie usług chmury obliczeniowej

1.18. **ZARZĄDZANIE BEZPIECZEŃSTWEM**

- 1.18.1. Zapewniony jest udokumentowany model bezpieczeństwa Systemu
- 1.18.2. Zapewnione są zdefiniowane i opisane funkcje zarządzania bezpieczeństwem Systemu
- 1.18.3. Zapewniona jest pełna identyfikowalność zmian parametrów i reguł Systemu
- 1.18.4. Zapewniona jest możliwość ograniczenia dostępu użytkownika do określonych danych (w zależności od funkcji)
- 1.18.5. Zapewnione jest 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
- 1.18.6. Zapewniona jest 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.
- 1.18.7. Zapewniona jest dokumentacja opisująca zasady bezpiecznego użytkowania Systemu z punktu widzenia użytkownika oraz administratora
- 1.18.8. System musi gwarantować pełną kontrolę administracyjną minimum w zakresie:
 - 1.18.8.1. rejestracji zmian konfiguracji
 - 1.18.8.2. rejestracji dokonywania poprawek
 - 1.18.8.3. rejestracji uaktualnień Systemu.
- 1.18.9. MUSI zostać zapewniona możliwość konfiguracji z poziomu administracyjnego różnorodnych mechanizmów uwierzytelniania (SSO, bez SSO, dodatkowe stopnie uwierzytelnienia np. SMS/token) w oparciu o przynależność do odpowiednich grup.
- 1.18.10. System MUSI mieć możliwość nadawania uprawnień do transakcji/funkcjonalności systemu oraz do danych i wynikowe uprawnienia mają być logicznym iloczynem uprawnień do danych i funkcji.
- 1.18.11. System MUSI mieć możliwość przeprowadzenia przekrojowych analiz uprawnień użytkowników lub grup użytkowników.
- 1.18.12. 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)
- 1.18.13. 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)

- 1.18.14. 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.
- 1.18.15. 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.
- 1.18.16. 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.
- 1.18.17. Procedura ustawiania hasła dla klientów zewnętrznych 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.
- 1.18.18. Zapewnione jest miejsce do przechowywania informacji na temat audytu / logów (np. tabele logów, pliki logów)
- 1.18.19. Zapewniona jest możliwość czasowego ustawienia śledzenia w Systemie wszystkich aktywności użytkowników i administratorów
- 1.18.20. Zapewnione jest posiadanie przez każdą transakcję / operację swojego identyfikatora / numeru referencyjnego specyficznego dla Systemu, umożliwiającego identyfikację ciągu zdarzeń w systemie w celach rekonyliacji i audytu
- 1.18.21. Zapewniony jest dostęp do raportów o logowaniach i działaniach użytkowników
- 1.18.22. Zapewniony jest dostęp do raportów o wszelkich nieudanych próbach logowania
- 1.18.23. Zapewniony jest dostęp do rejestrów zawierających opis błędów, które wystąpiły w systemie (stack trace)
- 1.18.24. Rozwiązanie MUSI zapewnić mechanizmy weryfikacji integralności danych, plików konfiguracyjnych i krytycznych obszarów Systemu
- 1.18.25. Wymagane jest zapewnienie mechanizmów audytowych, rejestrujących 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:
 - 1.18.25.1. konfigurowalna wielkość dziennika transakcji z możliwością automatycznej archiwizacji
 - 1.18.25.2. reglamentowany dostęp do dziennika dla wybranych grup osób
- 1.18.26. Wymagany jest interfejs GUI do przeglądania i analizy zapisów w logu audytowym.
- 1.18.27. Wymagana jest możliwość eksportowania zapisów z logów audytowych do plików o ustalonej strukturze (pliki płaskie, csv, xml).
- 1.18.28. 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"
- 1.18.29. 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.

- 1.18.30. Każda operacja wykonana w Systemie musi być przypisana do konkretnego identyfikatora użytkownika.
- 1.18.31. 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.
- 1.18.32. Zapewniona jest możliwość generowania raportów odnośnie przetwarzanych danych osobowych (konkretnej osoby) minimum w zakresie:
 - 1.18.32.1. uzyskania informacji jakie szczegółowe dane osobowe są zebrane w Systemie
 - 1.18.32.2. uzyskania informacji od kiedy są przetwarzane dane (włączając informacje o zgodzie użytkownika)
 - 1.18.32.3. uzyskania informacji o źródle, z którego pochodzą dane (użytkownik Systemu lub system zewnętrzny)
 - 1.18.32.4. uzyskania informacji do jakich zewnętrznych systemów dane są udostępniane/przekazywane
- 1.18.33. Zapewnione jest wsparcie Dostawcy Systemu w przeprowadzeniu przez Zamawiającego (zewnętrznego lub wewnętrznego) audytu bezpieczeństwa rozwiązania (w tym testów penetracyjnych wykrywających podatności Systemu) przed produkcyjnym uruchomieniem
- 1.18.34. Zapewniona jest 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
- 1.18.35. 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
- 1.18.36. Strefa DMZ powinna być zabezpieczona zaporami sieciowymi (firewall) zarówno od strony Systemu jak i od strony innych sieci. Reguły na zaporach powinny pozwalać jedynie na konkretne połączenia do DMZ z sieci wewnętrznej Systemu oraz z innych sieci. Zapory sieciowe powinny 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
- 1.18.37. Dozwolony jest jedynie ruch inicjowany z sieci wewnętrznej Systemu w kierunku strefy DMZ a zabroniony jest jakikolwiek ruch sieciowy inicjowany w kierunku odwrotnym
- 1.18.38. Serwery w strefie DMZ powinny zawierać jedynie wybrane dane z systemów wewnętrznych i jeśli to możliwe funkcjonalnie dane te powinny być jedynie do odczytu
- 1.18.39. System musi zapewniać wsparcie dla silnego uwierzytelniania wieloskładnikowego z wykorzystaniem centralnego PKI w GK PGE. Dostęp zdalny do zasobów wewnętrznych będzie realizowany dodatkowo poprzez systemy VPN
- 1.18.40. Zapewniona jest separacja dostępu (wykorzystanie różnych komponentów warstwy prezentacji/serwerów WWW) dla użytkowników wewnętrznych oraz zewnętrznych, łączących się z internetu
- 1.18.41. Zapewnione jest wsparcie Dostawcy Systemu w procesie testowania i dopuszczania nowych wersji aplikacji webowej zabezpieczonej firewallem aplikacyjnym (Web Application Firewall)

- 1.18.42. Sesja dostępu zdalnego Dostawcy do komponentu Systemu w trybie administracyjnym będzie rejestrowana w dedykowanym komponencie bezpieczeństwa.
- 1.18.43. Zapewnione są zintegrowane mechanizmy wykonywania i przywracania kopii zapasowych wszystkich tabel, plików i innych informacji (np. konfiguracji)
- 1.18.44. Zapewniona jest 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
- 1.18.45. Zapewniony jest zintegrowany dostęp do zarchiwizowanych danych Systemu
- 1.18.46. System MUSI umożliwiać realizowanie kopii danych Systemu w technologii „on-line” z wykorzystaniem automatycznych narzędzi do jej planowania i przeprowadzania.
- 1.18.47. System musi umożliwiać odtwarzanie kopii danych do punktu w czasie + dane z logów transakcyjnych.
- 1.18.48. Zapewnione jest narzędzie do ciągłego monitorowania pracy systemu i automatycznego powiadamiania administratorów systemu w przypadku wystąpienia problemów
- 1.18.49. 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)
- 1.18.50. Zapewnione zostaną odpowiednie procedury bezpiecznej aktualizacji oprogramowania, korekt błędów i innych modyfikacji Systemu.
- 1.18.51. System POWINIEN posiadać wewnętrzne mechanizmy wykrywania błędów funkcjonowania Systemu i ich rejestrację w dzienniku.
- 1.18.52. System musi wykonywać funkcję automatycznego powiadamiania administratora (w formie komunikatów) o wystąpieniu błędu bezpośrednio na konsolę administracyjną (log błędów na ekranie).
- 1.18.53. System musi wykonywać funkcję automatycznego powiadamiania administratora (w formie komunikatów) o wystąpieniu błędu poprzez e-mail.
- 1.18.54. System musi gwarantować możliwość wykonywania kopii rezerwowych bez potrzeby wstrzymania pracy w Systemie.
- 1.18.55. Rozwiązanie musi posiadać udokumentowane i przetestowane procedury przywracania Systemu po awarii dowolnego komponentu Systemu.
- 1.18.56. System musi posiadać narzędzia do monitorowania ogólnej wydajności Systemu. Raporty z tego narzędzia będą dostępne dla administratorów Systemu.
- 1.18.57. Dla Systemu MUSZĄ być uzgodnione pomiędzy Dostawcą i Zamawiającym poziom RPO i czas RTO dla uzgodnionego minimalnego poziomu działania usług biznesowych MBCO
- 1.18.58. Oferent w każdym aspekcie dostępu do danych/informacji powinien dążyć do 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.

- 1.18.59. Proces wytwarzania Systemu powinien być zgodny z Normami ISO/IEC 27001 Zarządzanie Bezpieczeństwem Informacji (np. zapewnienie poufności kodu źródłowego)
- 1.18.60. Proces wytwarzania Systemu powinien stosować najlepsze praktyki programistyczne w zakresie bezpieczeństwa (analiza kodu, weryfikacja stosowanych bibliotek itp.)
- 1.18.61. Proces wytwarzania Systemu powinien wykorzystywać preferowane nowoczesne metody autentykacji z pominięciem hasła tzw. „password-less”