1. WYMAGANIA BEZPIECZEŃSTWA

***Skróty użyte na potrzeby niniejszego dokumentu:***

|  |  |  |
| --- | --- | --- |
| ***ADFS*** | - Active Directory Federation Services (ang.) – usługa bezpiecznego udostępniania tożsamości cyfrowej z zaufanymi partnerami | |
| ***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 | |
| ***CSP*** | - Cloud Service Provider (ang.) – dostawca usług w chmurze | |
| ***DMZ*** | - 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 | |
| ***MBCO*** | | - Minimum Business Continuity Objective - minimalny poziom odtworzenia usługi teleinformatycznej, który jest akceptowalny dla Spółki do osiągnięcia jej celów biznesowych w sytuacji krytycznej |
| ***MFA*** | | - Multi Factor Authentication (ang.) - Uwierzytelnianie wieloskładnikowe, metoda uwierzytelniania, która wymaga od użytkownika podania co najmniej dwóch niezależnych czynników (np. 2FA z hasłem jednorazowym) w celu potwierdzenia tożsamości. Te czynniki mogą obejmować coś, co użytkownik wie (np. hasło), coś, co posiada (np. telefon), oraz coś, co jest unikalne dla użytkownika (np. odcisk palca, PIN, token sprzętowy lub programowy) |
| ***PCD*** | - Plan Ciągłości Działania | |
| ***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 | |
| ***RCB*** | - Rządowe Centrum Bezpieczeństwa, opracowania i zalecenia w kontekście Narodowego Programu Ochrony Infrastruktury Krytycznej | |
| **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) | |
| ***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 | |
| ***SaaS*** | - Software as a Service (ang.) – oprogramowanie świadczone jako usługa w chmurze obliczeniowej | |
| ***SIEM*** | - Security Information and Event Management (ang.) – zarządzanie informacjami i zdarzeniami bezpieczeństwa | |
| ***SLA*** | - Service Level Agreement (ang.) – umowa o gwarantowanym poziomie świadczenia usług | |
| ***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 | |
| ***uKSC*** | - ustawa o Krajowym Systemie Cyberbezpieczeństwa | |
| ***URI*** | - Uniform Resource Identifier (ang.) – ujednolicony identyfikator jednoznacznie wskazujący na zasób | |
| ***XSS*** | - Cross Site Scripting – możliwości osadzenia kodu w treści atakowanej strony | |

***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. |
| ***Plan Ciągłości Działania*** – zbiór Planów Awaryjnych, procedur odtworzenia usług na wypadek awarii, Instrukcji technicznych, Scenariuszy Awarii oraz mapy powiązań pomiędzy nimi opracowany dla Systemu, zapewniający dotrzymanie uzgodnionych parametrów usługi. |
| ***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. |
| ***Ransomeware* –** oprogramowanie, które blokuje dostęp do Systemu lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego |
| ***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 nierozerwalną 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. 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. Muszą ku temu zaistnieć szczególne okoliczności lub uzasadnione powody zatwierdzone przez Zamawiającego

* + 1. ZALECANE jest unikanie zakupu rozwiązań informatycznych pochodzących z krajów prowadzących nieprzychylną lub wrogą politykę wobec Rzeczpospolitej Polskiej, krajów objętych sankcjami Rady Bezpieczeństwa ONZ 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 MUSZĄ być zamieszczone informacje na temat konfiguracji i mechanizmów w Systemie realizujących wymagania opisywane poniżej.

1.2.2.1 Ogólny opis i relacje pomiędzy poszczególnymi komponentami Systemu *(\*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS)*

1. wyszczególnione segmenty sieci tzn. DMZ, strefa chroniona, Internet itp. oraz osadzenie tych komponentów w poszczególnych strefach
2. 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.

1.2.2.2 Opisane poszczególne komponenty w zakresie:

a. mechanizmy tworzenia i odtwarzania kopii zapasowej z określonymi czasami trwania operacji *(\*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS)*,

b. procedury przywracania po katastrofie *(\*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS)*,

1. procedury aktualizacji oprogramowania *(\*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS)*,
2. na jakich Kontach są uruchamiane usługi i z jakimi uprawnieniami *(\*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS)*,
3. mechanizmy Kontroli stanu Systemu,
4. w jaki sposób jest realizowany dostęp serwisowo-administracyjny *(\*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS)*,
5. wykorzystywane Konta techniczne *(\*wymaganie nie dotyczy wewnętrznych komponentów usług SaaS)*,
6. zarządzanie Kontami w szczególności w zakresie ważności, wygasania,
7. możliwości udostępniania zarządzania Kontami do zewnętrznego Systemu IAM,
8. dostępnych metod uwierzytelniania Użytkowników i innych Systemów wchodzących w skład rozwiązania,
9. polityki haseł lub innych środków uwierzytelnienia,
10. zastosowanych mechanizmów autoryzacji Użytkowników i komponentów współpracujących, m. audytu działań i operacji w Systemie,
11. wykorzystywanego mechanizmu logowania i możliwości podłączenia do zewnętrznego Systemu

SIEM,

1. mechanizmów synchronizacji czasu (*\*zapewnienia* *spójności danych w kontekście aktualnego czasu)*,
2. 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 lub równoważnymi. Wymaganie nie dotyczy elementów Systemu w postaci stacji roboczych, urządzeń mobilnych korzystających z tego Systemu jako usługi:

1.3.1.1 Normą ISO/IEC 27001:2022 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 Dla Systemów przetwarzających, w ocenie Zamawiającego, istotne dane (np. dane osobowe), MUSI być stosowane pełne szyfrowanie danych mocnymi algorytmami zarówno w spoczynku jak i w trakcie ich przesyłania.

1.3.4 Dla Systemu MUSZĄ być opracowane procedury przywracania po katastrofie *(\*wymaganie nie dotyczy usług SaaS dla których istotne są parametry SLA)*.

1.3.5 System POWINIEN posiadać co najmniej dwa środowiska: produkcyjne i testowe. System POWINIEN mieć dodatkowo środowiska preprodukcyjne i rozwojowe.

1.3.6 Dla Systemu MUSZĄ zostać zdefiniowane parametry RTO, RPO na okoliczność wystąpienia awarii usługi *(\*wymaganie nie dotyczy usług SaaS dla których istotne są parametry SLA)*.

1.3.7 System NIE MOŻE posiadać pojedynczego punktu awarii („No Single Point of Failure”).

1.3.8 System POWINIEN mieć dostępne mechanizmy tworzenia i odtwarzania kopii zapasowej z określonymi czasami trwania operacji.

**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.

1.4.12 Aktualizacje i nowe wersje subkomponentów Systemu MUSZĄ zostać poddane weryfikacji na obecność malware i nieautoryzowanej modyfikacji przed instalacją w komponentach docelowych Zamawiającego

**1.5 RUCH SIECIOWY**

1.5.1 System POWINIEN być umieszczony w wydzielonym segmencie sieci fizycznej lub logicznej (VLAN).

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 Segment sieci wydzielony dla Systemu POWINIEN mieć adresację z jednej z klas adresowych zarezerwowanych dla prywatnych sieci lokalnych (RFC 1918/RFC4193).

1.5.6 Komunikacja Systemu z innymi Systemami lub Użytkownikami POWINNA się odbywać za pomocą serwera pośredniczącego (Reverse Proxy). W przypadku ruchu przychodzącego z sieci niezaufanych ruch ten MUSI się odbywać za pomocą serwera pośredniczącego (Reverse Proxy).

1.5.7 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.

1.5.8 Wszystkie usługi Systemu MUSZĄ być w sieci jednoznacznie identyfikowane. Do identyfikacji ZALECANE jest wykorzystanie certyfikatów cyfrowych.

1.5.9 Wymagany ruch sieciowy MUSI być opisany w sposób zgodny z wewnętrznym szablonem Zamawiającego.

1.5.10 Ruch sieciowy przed przekazaniem do realizacji podlega procesowi kontroli zgodności z architekturą Systemu i akceptacji przez Zamawiającego.

1.5.11 Szablon 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).

1.5.12 Aktualny szablon z ruchem sieciowym służy jako wsad do dokumentacji technicznej Systemu oraz powykonawczej Dokumentacji Bezpieczeństwa.

**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/TLS POWINIEN stosować aktualne zalecenia NIST 800-131A, przykładowo:

a. algorytm wymiany kluczy: DH/ECDHE, RSA,

b. algorytm uwierzytelniania: ECDSA, RSA

c. długość klucza RSA co najmniej 2048, ECDSA co najmniej 256

d. symetryczny algorytm szyfrowania: AES-256

e. funkcje skrótu: SHA-2, SHA-256.

f. rekomendowane użycie wersji TLS 1.3

1.6.4 System do transmisji danych poprzez tunel VPN POWINIEN stosować protokół IPSec z parametrami uznanymi za obecnie dopuszczalne (nieprzestarzałe), np. opisane w NIST.SP.800-77 przykładowo:

a. tryb pracy: ESP w trybie tunelowym,

b. protokół negocjacji parametrów: IKE,

c. metoda uwierzytelniania stron: certyfikaty cyfrowe,

d. symetryczny algorytm szyfrowania: AES- 256

e. funkcje skrótu: SHA-2, SHA-256,

f. grupa Diffie-Hellman: Group 19 lub wyższa, preferowana 24

g. tryb negocjacji w fazie I: Main mode, Aggresive 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 lub udokumentowany brak podatności w tym zakresie.

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 lub udokumentowany brak podatności w tym zakresie.

1.6.5.7 Usługa udostępniana po protokole http lub https MUSI być dostępna odpowiednio na portach 80 i 443 TCP. Dostęp do usługi na porcie HTTP MUSI automatycznie przekierowywać komunikację na port HTTPS.

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) lub udokumentowany brak podatności w tym zakresie.

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, co najmniej: 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,

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 pewien okres (np. 10 minut) lub należy zastosować inne mechanizmy ochrony (np. Capcha).

1.7.5 Konta użytkowników wykorzystywane w usłudze muszą być imienne, tzn. niewspółdzielone.

1.7.6 Usługa musi mieć zdefiniowaną procedurę resetu hasła dla kont nieobjętych funkcjonalnością SSO.

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 lub udokumentowany brak podatności w tym zakresie.

**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. Odnośnie danych osobowych powinny zostać zanonimizowane w dopuszczalnym zakresie.

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 Zamawiającego. System do uwierzytelnienia Użytkownika POWINIEN korzystać z mechanizmu Kerberos lub NTLMv2 udostępnionych przez korporacyjne Active Directory lub stosować dopuszczalne metody uwierzytelniania bezhasłowego tzw. passwordless lub nowoczesnych metod uwierzytelniania SAML/ADFS wykorzystując zarazem funkcję jednokrotnego logowania tzw. SSO.

1.9.5 System NIE POWINIEN wykorzystywać mechanizmów uwierzytelniania wymagających przesłania do Systemu Hasła Użytkownika. Zalecane jest wykorzystanie protokołu „Secure Remote Password” (RFC 2945/RFC 5054)

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 aktualnie stosowanymi najlepszymi praktykami, przykładowo minimalna długość hasła użytkownika 12 znaków, administratora 15 znaków lub stosować silne metody uwierzytelniania.

W zakresie haseł dla Klientów Systemu (Użytkownik zewnętrzny), powinna być możliwość:

* ustalenia odrębnych zasad niż dla użytkowników Zamawiającego;
* wyłączenia wymuszenia zmiany hasła;
* zastosowania komunikatu informującego o dobrych praktykach dotyczących haseł, zaleceniach jego zmiany i ryzyku związanym z zapamiętywaniem haseł na urządzeniach końcowych i w przeglądarkach (a w przypadku zapamiętywania, o potrzebie stosowania dodatkowych zabezpieczeń w dostępie do tych urządzeń: PIN/Hasło, odcisk palca itp.).

1.9.9 System POWINIEN wymuszać na Użytkownikach okresowe zmiany Hasła dla kont nieobjętych SSO.

1.9.10 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).

1.9.11 Po pierwszym udanym uwierzytelnieniu Użytkownika w Systemie, administracyjnym odblokowaniu konta, administracyjnej zmianie hasła , System POWINIEN wymusić zmianę Hasła przed udostępnieniem mu jakiejkolwiek innej funkcjonalności. Mechanizm wymuszania zmiany hasła powinien być możliwy do włączenia na koncie przez administratora - dotyczy kont nietechnicznych oraz nieobjętych SSO.

1.9.12 System MUSI posiadać udokumentowane procedury zmiany haseł dla kont technicznych.

1.9.13 System POWINIEN wspierać i udostępniać możliwość wykorzystania mechanizmów jednokrotnego uwierzytelniania SSO (Single Sign On) dla użytkowników wewnętrznych, uwierzytelniających się w korporacyjnej domenie Active Directory.

1.9.14 System MUSI zapewniać mechanizmy pozwalające na zarządzanie danymi uwierzytelniającymi, tj. nadawaniem, zmianą, ponownym ustawieniem, czasem ważności.

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 autoryzacji 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 *(\*wymaganie nie dotyczy usług SaaS)*

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 sekundy,

c. Identyfikator Użytkownika wykonującego operację,

d. adres IP, z którego wykonano operację,

e. informację o pomyślnym zakończeniu operacji lub kodu zwróconego błędu w przypadku niepowodzenia.

1.11.4 W przypadku każdej (zarówno udanej jak i nieudanej) próby uwierzytelnienia System MUSI rejestrować następujące informacje:

1. czas wykonania próby uwierzytelnienia z dokładnością sekundy,
2. wprowadzony Identyfikator Użytkownika,
3. adres IP, z którego wykonano próbę,
4. 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:

1. czas wykonania operacji z dokładnością sekundy,
2. Identyfikator Użytkownika lub dane pozwalające na identyfikację Sesji Użytkownika,
3. adres IP, z którego wykonano operację,
4. kod, symbol lub pełny opis operacji wykonanej przez Użytkownika,
5. obiekt lub komponent, którego operacja dotyczy,
6. wszelkie argumenty lub dane użyte lub przekazane do Systemu podczas operacji,
7. informacja o pomyślnym zakończeniu operacji lub kod zwróconego błędu w przypadku niepowodzenia.

1.11.6 System POWINIEN mieć możliwość podłączenia do Systemu SIEM Zamawiającego. System POWINIEN mieć możliwość takiej konfiguracji, aby do Systemu SIEM mogły być logowane następujące informacje (związane z czynnościami na rzecz Zamawiającego):

1. błędy Systemu,
2. operacje uwierzytelnienia (udane i nieudane),
3. operacje nadawania i odbierania dostępu (MAC, RBAC, DAC)
4. próby nieautoryzowanego dostępu do Zasobów,
5. informacje o możliwej awarii,
6. otwarcie oraz zamknięcie – w tym automatyczne - sesji Użytkownika w Systemie
7. zmiany w konfiguracji Systemu.

1.11.7 Preferowanym protokołem przekazywania zdarzeń do SIEM z systemów jest protokół Syslog (RFC 5424).

1.11.8 Usługa MUSI mieć włączone logowanie zdarzeń z retencją co najmniej 180 dni w zakresie

1. operacji uwierzytelniania, poprawnego i niepoprawnego
2. operacji nadawania i odbierania uprawnień
3. istotnych operacji w systemie związanych z działaniem użytkownika usługi
4. operacji zablokowania konta w przypadku wielokrotnego błędnego uwierzytelnienia
5. 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**

1.13.1 Jeżeli w Systemie przetwarzane są Dane Osobowe to MUSI być on zgodny z przepisami o ochronie danych osobowych, a w szczególności:

1. Zapewnić możliwość realizacja Praw jednostki dla Danych Osobowych przetwarzanych w tym systemie, w tym:
   1. Prawo dostępu (i uzyskania kopii danych) – Art. 15 RODO
   2. Prawo do sprostowania danych - Art. 16 RODO
   3. Prawo do usunięcia danych ("prawo do bycia zapomnianym") – ART.17 RODO
   4. Prawo do ograniczenia przetwarzania – Art. 18 RODO
   5. Prawo do przenoszenia danych – Art. 20 RODO
   6. Prawo do sprzeciwu – Art. 21 RODO
2. Zapewnić spełnianie wymogu Minimalizacja danych, czyli:
   1. Przetwarzamy tylko dane niezbędne do realizacji celu przetwarzania
   2. 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.)

**1.14 KRYPTOGRAFIA**

Dopuszczalne są standardy kryptograficzne (symetryczne, asymetryczne, podpisu cyfrowego) aktualnie uznane za rekomendowane (nieprzestarzałe), np. w oparciu o publikację NIST.SP.800-175B:

1.14.1 Dopuszczalne są następujące standardy szyfrowania symetrycznego:

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

Zalecane tryby to GCM, CFB, OFB, CTR, CBC z wykorzystaniem wektora inicjalizującego (IV – Initialization

Vector) generowanego za każdym razem z zachowaniem poufności.

1.14.2 Dopuszczalne są następujące standardy szyfrowania asymetrycznego:

|  |  |
| --- | --- |
| Algorytm | Długość klucza |
| RSA | 2048 bitów i wzwyż |
| ECC | 256 bitów 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 | 256 bitów i wzwyż |
| DSA | 2048 bitów i wzwyż |

1.14.6 Klucze kryptograficzne służące do zabezpieczenia danych MUSZĄ być generowane lokalnie w infrastrukturze HSM Zamawiającego.

**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:

1. Injection - możliwości wstrzykiwania nieautoryzowanych komend w przekazywanych parametrach do aplikacji,
2. Broken Authentication and Session Management - możliwości przechwytywania haseł oraz identyfikatorów sesji, zarówno podczas transmisji oraz ich przechowywania,
3. Cross Site Scripting (XSS) – możliwości osadzenia kodu w treści atakowanej strony,
4. Insecure Direct Object References – możliwości bezpośredniego nieautoryzowanego odwoływania się do obiektów poprzez modyfikację parametrów,
5. Security Misconfiguration - błędów w konfiguracji w postaci:
6. braków w aktualizacji komponentów,
7. niewyłączenia nieużywanych usług, kont, stron, portów,
8. braku zamiany domyślnych haseł,
9. wyświetlania kodu błędów oraz stosu wywołań w przypadku wystąpienia błędu aplikacji,
10. 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,

1. Missing Function Level Access Control – błędów w aplikacji w postaci:
2. braku ograniczenia dostępu w przypadku nieuwierzytelniania,
3. braku ograniczenia dostępu do zasobów zawierających dane konfiguracyjne, logi zdarzeń, pliki źródłowe,
4. braku ograniczenia dostępu do zasobów w zależności od uprawnień,
5. Cross-Site Request Forgery (CSRF) – możliwości przesyłania naturyzowanych żądań do aplikacji,
6. Using Components with Known Vulnerabilities – używania komponentów, modułów i bibliotek ze znanymi podatnościami,
7. 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:

1. NIE MOŻE być krótszy niż 128 bitów,
2. MUSI być losowy,
3. MUSI być generowany z jak najszerszego zestawu znaków,
4. MUSI być unikatowy dla Użytkowników danej aplikacji,
5. MUSI być zmieniany/generowany przy uwierzytelnieniu Użytkownika,
6. MUSI być zmieniany/deaktywowany przy wylogowaniu Użytkownika
7. MUSI być zmieniany/generowany przy przejściu pomiędzy HTTP i HTTPS,
8. POWINIEN być akceptowany za poprawny tylko ten identyfikator, który został wygenerowany przez aplikację,
9. MUSI być unieważniany po określonym czasie bezczynności Użytkownika,
10. 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,
11. NIE MOŻE być ujawniany w komunikatach błędów i logach,
12. MUSI być unieważniany i zmieniany lub usuwany przy wylogowaniu Użytkownika,
13. NIE MOŻE być zapamiętywany w przeglądarce (brak funkcji zapamiętaj mnie),
14. 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 być 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. 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 lub udokumentowany brak podatności w tym zakresie.

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 *(\*wymaganie uchylone, niestosowane w nowoczesnych przeglądarkach)*.

1.15.13 Udostępniane przez aplikację po HTTPS strony MUSZĄ mieć zdefiniowany nagłówek StrictTransport-Security. Nagłówek POWINIEN mieć następującą postać: Strict-Transport-Security: maxage=31536000; includeSubDomains

1. wartość max-age=31536000 wymusza, że wszelkie zapytania w przyszłości określonej przez max-age do danej witryny muszą obywać się po HTTPS,
2. 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 lub posiadać udokumentowany brak podatności w tym zakresie.

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:

1. Normą ISO/IEC 27001:2022 Zarządzanie Bezpieczeństwem Informacji
2. Normą ISO 22301 Zarządzanie Ciągłością Działania
3. Normą ISO 27017 Bezpieczeństwo Informacji dla usług w Chmurze
4. Normą ISO 27018 Ochrona Danych Osobowych w Chmurze
5. Normą ISO 27701 Zarządzanie i ochrona danych osobowych w chmurze obliczeniowej

1.16.2 Wymagane jest wykorzystanie przez Dostawcę najlepszych praktyk branżowych:

1. CSA – ang. Cloud Security Alliance certyfikacja STAR ang. Security Trust Assurance and Risk (https://www.bsigroup.com/pl-PL/Certyfikacja-CSA-STAR/ ). Wymagane jest zapewnienie przez Dostawcę raportu potwierdzającego zgodność zabezpieczeń z aktualną macierzą kontroli (ang. CSA CCM Self-Assessment)
2. CIS – ang. Center for Internet Security (zalecenia kontrolne/benchmarki, utwardzanie systemów, w szczególności dla rozwiązań chmurowych „CIS Cloud Companion”)
3. OWASP – ang. Open Web Application Security Project
4. ASVS – ang. Application Security Verification Standard (standardowo Level 2, natomiast gdy dotyczy infrastruktury krytycznej – Level 3)
5. Dobrych praktyk i rekomendacji wydanych przez Rządowe Centrum Bezpieczeństwa w Narodowym Programie Ochrony Infrastruktury Krytycznej w kontekście uruchamiania usług w chmurze publicznej

1.16.3 System MUSI być zgodny 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 POWINIEN dokładać wszelkich najlepszych starań, aby zapewnić danym/informacji: poufność, integralność, dostępność oraz rozliczalność. Zarówno w obszarach przechowywania danych, jak i podczas ich transportu pomiędzy różnymi środowiskami „Systemu” lub integracji z innymi „Systemami”. Należyta dokładność POWINNA być stosowana już na etapie analizy rozwiązań chmurowych, jak i w trakcie projektowania oraz realizacji rozwiązań.

1.16.6 System MUSI wspierać sposób uwierzytelnienia przez ADFS Zamawiającego lub Azure AD/Entra ID.

1.16.7 System 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 Dla usług niewymagających dostępu publicznego wymaga się wykorzystania dostępu warunkowego dopuszczającego dostęp do usługi wyłącznie z infrastruktury Zamawiającego w uzgodniony optymalny sposób, np.:

1. Filtrowanie ruchu IP na zaporach sieciowych
2. Zastosowanie tunelowania IPSec VPN pomiędzy CPD Zamawiającego a środowiskiem chmurowym
3. Zastosowanie minimum 2FA/MFA w przypadku braku innych możliwości

1.16.12 Wymaga się zgodności modelu przetwarzania danych z rekomendacjami Rządowego Centrum Bezpieczeństwa opisanymi w Załączniku 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej, ze szczególnym uwzględnieniem pkt. 2.8.3.2

1.16.13 Preferowane jest wykorzystanie uniwersalnej warstwy abstrakcji uniezależniającej się od dostawcy chmury, np.:

1. Zastosowanie konteneryzacji
2. Zastosowanie wirtualizacji VMWare on Cloud
3. Wsparcie dla oprogramowania firm trzecich przeprowadzających migrację pomiędzy dostawcami chmur obliczeniowych
4. Zastosowanie w Systemie funkcjonalności IaC and. Infrastructure as a Code

1.16.14 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 *(\*wymaganie dotyczy udokumentowania komponentów odpowiednio dla standardu modelu odpowiedzialności dla usług chmurowych CSP/Wykonawca/Zamawiający)*

1.17.2 Uruchomienie uwierzytelniania dwuskładnikowego (2FA) do usług chmurowych (dostęp typu back office) z udziałem ADFS Zamawiającego jako iDP (ang. Identity Provider) i stosowanymi mechanizmami jednokrotnego logowania SSO

1.17.3 Wykorzystanie w procesie nadawania uprawnień systemu IAM Zamawiającego

1.17.4 Przesyłanie incydentów i zdarzeń bezpieczeństwa do systemów Zamawiającego (rekomendowana integracja zdarzeń po stronie chmury z systemami Zamawiającego SIEM/SOAR).

1.17.5 Zapewnienie odrębnej kopii zapasowej danych Systemu w infrastrukturze Zamawiającego (np. integracja z systemem kopii zapasowych Zamawiającego lub okresowe eksporty danych)

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-premisess” , migrację do innego dostawcy lub inne scenariusze biznesowe.

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

1.18.  **ZGŁASZANIE INCYDENTÓW BEZPIECZEŃSTWA**

1.18.1 Dostawca zobowiązany jest do bezzwłocznego informowania Zamawiającego o:

1.18.1.1 zauważonym przypadku naruszenia bezpieczeństwa systemów i zasobów

teleinformatycznych, mających wpływ lub będących w zakresie świadczonych usług

1.18.1.2 wykryciu podatności lub luki w zabezpieczeniach usług/Systemu,

1.18.1.3 stwierdzonym przypadku naruszenia integralności sprzętu, oprogramowania bądź podejrzeniu próby takiego naruszenia,

1.18.1.4 stwierdzonym przypadku infekcji szkodliwym oprogramowaniem stacji roboczej, z której inicjowany jest dostęp do usługi/Systemu,

1.18.1.5 podejrzeniu utraty poufności indywidualnych danych uwierzytelniających

1.18.2 Dostawca zobowiązuje się do informowania Zamawiającego o wykrytych incydentach bezpieczeństwa dot. danych powierzonych do przetwarzania przez Zamawiającego (np. wielokrotne nieudane próby logowania, lub wykrycie złośliwej zawartości) oraz o atakach na systemy inne Wykonawcy, gdy używa infrastruktury połączonej z Zamawiającym (skomunikowanej z innymi usługami Zamawiającego)

1.19  **WYMAGANIA UZUPEŁNIAJĄCE DLA USŁUG KLUCZOWYCH**

1.19.1 MUSI być zapewniony udokumentowany model bezpieczeństwa Systemu

1.19.2 MUSI być zapewniona możliwość automatycznego wylogowania użytkownika z Systemu w przypadku braku aktywności w sesji (brak aktywności w określonymi 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.

1.19.3 MUSI być zapewniona dokumentacja opisująca zasady bezpiecznego użytkowania Systemu z punktu widzenia użytkownika oraz administratora

1.19.4 System MUSI gwarantować pełną kontrolę administracyjną minimum w zakresie:

1. rejestracji zmian konfiguracji
2. rejestracji dokonywania poprawek
3. rejestracji uaktualnień Systemu.

1.19.5 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.

1.19.6 MUSI być zapewniona Integralność danych podczas przetwarzania i przechowywania przez System

1.19.7 MUSI być zapewniona ochrona wszystkich danych przed ich nieautoryzowanym usunięciem

1.19.8 MUSI być zapewniona dodatkowa autoryzacja użytkowników podczas modyfikowania istotnych parametrów Systemu i danych (np. podczas zmiany hasła)

1.19.9 System MUSI mieć możliwość przeprowadzenia przekrojowych analiz uprawnień użytkowników lub grup użytkowników.

1.19.10 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).

1.19.11 Dla użytkowników Systemu niepowiązanych z dostawcą tożsamości Zamawiającego 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, token sprzętowy).

1.19.12 System POWINIEN wspierać możliwość wykorzystania kwalifikowanego i niekwalifikowanego podpisu elektronicznego do autoryzowania dowolnych transakcji w Systemie.

1.19.13 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.

1.19.14 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.

1.19.15 MUSI być zapewniona funkcjonalność przeglądania audytu operacji (tworzenia, przeglądania, aktualizacji, usuwania) dla dedykowanej, uprawnionej grupy użytkowników.

1.19.16 MUSI być zapewniona możliwość czasowego ustawienia śledzenia w Systemie wszystkich aktywności użytkowników i administratorów.

1.19.17 MUSI być zapewnione posiadanie przez każdą transakcję / operację indywidualnego identyfikatora / numeru referencyjnego specyficznego dla Systemu, umożliwiającego identyfikację ciągu zdarzeń w Systemie w celach rekoncyliacji i audytu.

1.19.18 MUSI być zapewniony dostęp do raportów o logowaniach i działaniach użytkowników.

1.19.19 MUSI być zapewniony dostęp do raportów o wszelkich nieudanych próbach logowania.

1.19.20 MUSI być zapewniony dostęp do rejestrów zawierających opis błędów, które wystąpiły w systemie (ang. stack trace).

1.19.21 System MUSI zapewnić mechanizmy weryfikacji integralności danych, plików konfiguracyjnych i krytycznych obszarów Systemu

1.19.22 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

1.19.23 Wymagany jest interfejs graficzny do przeglądania i analizy zapisów logów audytowych.

1.19.24 Wymagana jest możliwość eksportowania zapisów z logów audytowych do plików o ustalonej strukturze (pliki płaskie, csv, xml).

1.19.25 Każda operacja wykonana w Systemie MUSI być przypisana do konkretnego identyfikatora użytkownika (w tym konta administratorów i techniczne).

1.19.26 Zmiany istotnych danych w Systemie (zakres uzgodniony z Zamawiającym na etapie wdrożenia) MUSZĄ być rejestrowane odrębnie w sposób pozwalający na określenie kto, kiedy i jakie dane zmienił wraz z informacją o poprzedniej ich zawartości.

1.19.27 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

1.19.28 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

1.19.29 Zapewniona MUSI być możliwość integracji Systemu z zewnętrznymi systemami typu SIEM poprzez definiowanie eksportu logów na każdym poziomie (systemowe, bazodanowe, aplikacyjne, audytowe itp.) do wskazanych kolektorów i z parametrami komunikacyjnymi konfigurowalnymi przez administratora

1.19.30 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

1.19.31 MUSI być zapewniona segmentacja (separacja fizyczna lub logiczna VLAN/VxLAN) pomiędzy komponentami różnych środowisk np. PROD/TEST

1.19.32 POWINNA być zapewniona separacja dostępów (wykorzystanie różnych komponentów warstwy prezentacji/serwerów WWW) dla użytkowników wewnętrznych oraz zewnętrznych, łączących się z internetu

1.19.33 MUSI być zapewnione wsparcie Wykonawcy Systemu w procesie testowania i dopuszczania nowych wersji aplikacji webowej zabezpieczonej firewallem aplikacyjnym (Web Application Firewall)

1.19.34 Sesja dostępu zdalnego Wykonawcy do komponentu Systemu w trybie administracyjnym będzie rejestrowana w dedykowanym komponencie bezpieczeństwa.

1.19.35 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.

1.19.36 MUSZĄ być zapewnione zintegrowane mechanizmy wykonywania i przywracania kopii zapasowych wszystkich tabel, plików i innych informacji (np. konfiguracji).

1.19.37 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.

1.19.38 MUSI być zapewniony zintegrowany dostęp do zarchiwizowanych danych Systemu.

1.19.39 System MUSI umożliwiać realizowanie kopii danych Systemu w technologii „on-line” z wykorzystaniem automatycznych narzędzi do jej planowania i przeprowadzania.

1.19.40 System MUSI umożliwiać odtwarzanie kopii danych do punktu w czasie + dane z logów transakcyjnych.

1.19.41 MUSI być zapewnione narzędzie do ciągłego monitorowania pracy systemu i automatycznego powiadamiania administratorów systemu w przypadku wystąpienia problemów.

1.19.42 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).

1.19.43 MUSZĄ być zapewnione odpowiednie procedury bezpiecznej aktualizacji oprogramowania, korekt błędów i innych modyfikacji Systemu.

1.19.44 System MUSI posiadać wewnętrzne mechanizmy wykrywania błędów funkcjonowania Systemu i ich rejestrację w dzienniku.

1.19.45 System MUSI wykonywać funkcję automatycznego powiadamiania administratora (w formie komunikatów) o wystąpieniu błędu bezpośrednio na konsolę administracyjną (log błędów na ekranie).

1.19.46 System MUSI wykonywać funkcję automatycznego powiadamiania administratora (w formie komunikatów) o wystąpieniu błędu poprzez e-mail.

1.19.47 System MUSI gwarantować możliwość wykonywania kopii rezerwowych bez potrzeby wstrzymania pracy w Systemie.

1.19.48 System MUSI posiadać udokumentowane i przetestowane procedury przywracania Systemu po awarii dowolnego komponentu Systemu.

1.19.49 System MUSI posiadać narzędzia do monitorowania ogólnej wydajności Systemu. Raporty z tego narzędzia będą dostępne dla administratorów Systemu.

1.19.50 Dla Systemu MUSZĄ być uzgodnione pomiędzy Wykonawcą i Zamawiającym poziom RPO i czas RTO dla uzgodnionego minimalnego poziomu działania usług biznesowych MBCO

1.19.51 Zabezpieczenie danych przetwarzanych w usłudze chmurowej (ang. In-transit) oraz przechowywanie danych w spoczynku (ang. at-rest) MUSI byc realizowane na podstawie kluczy szyfrujących generowanych w środowisku zamawiającego z wykorzystaniem HSM (ang. Hardware Security Module) Zamawiającego

1.19.52 Implementacja komponentów chmurowych wymaga opracowania planu wyjścia z usługi chmury obliczeniowej i zastąpienia jej innym rodzajem usługi lub zmianą dostawcy usług chmury obliczeniowej (również na wypadek awarii całej lokalizacji), bez uszczerbku dla zachowania zgodności działania z wymaganiami prawa i innych regulacji, w tym w szczególności związanych z udzielonymi licencjami lub zezwoleniami.

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

1.19.54 Zabezpieczenie kopii danych po stronie usług chmurowych MUSI być na co najmniej takim poziomie jak wymagane jest to dla rozwiązania on-premise (wymagania dla infrastruktury), w szczególności zastosowanie nadmiarowości komponentów, replikacji danych w ramach tego samego oraz zapasowego ośrodka CSP oddalonego co najmniej o 30km i odporne na ryzyka infekcji ransomeware

1.19.55 Dla usług chmurowych MUSZĄ być opracowane dedykowane procedury przywrócenia usługi po katastrofie uwzględnione w dokumentacji PCD (Plany Ciągłości Działania) z podziałem kompetencji i odpowiedzialności po stronach CSP/Dostawca/Zamawiający

1.19.56 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.

1.19.57 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 komponentów Systemu

1.19.58 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.

1.19.59 Proces wytwarzania Systemu MUSI być zgodny z Normami ISO/IEC 27001 Zarządzanie Bezpieczeństwem Informacji (np. zapewnienie poufności kodu źródłowego).

1.19.60 Proces wytwarzania Systemu MUSI stosować zalecenia fundacji OWASP „Open Web Application Security Project” oraz wykorzystać wstępne testowanie wg aktualnych zaleceń ASVS "Application Security Verification Standard".

1.19.61 Proces wytwarzania Systemu MUSI stosować najlepsze praktyki programistyczne w zakresie bezpieczeństwa (analiza kodu, weryfikacja stosowanych bibliotek itp.).

1.19.62 Proces wytwarzania Systemu POWINIEN wykorzystywać preferowane nowoczesne metody uwierzytelniania i autoryzacji z pominięciem hasła tzw. „password-less”.

1.19.63 Aktualizacje i nowe wersje subkomponentów Systemu MUSZĄ zostać poddane weryfikacji na obecność malware i nieautoryzowanej modyfikacji przed instalacją w komponentach docelowych Zamawiającego

1.19.64 System MUSI zapewniać funkcjonalność zdefiniowania retencji informacji przetwarzanych i przechowywanych w ramach Systemu, tak aby informacje dla których nie ma potrzeby ich przechowywania mogły być automatycznie usuwane (w szczególności dotyczy to danych osobowych).

1.19.65 System MUSI zapewniać funkcjonalność maskowania poufnych danych (w szczególności dotyczy to danych osobowych)

1.19.66 System MUSI zapewniać funkcjonalność pseudonimizacji/anonimizacji poufnych danych (np. podczas migracji danych do środowiska testowego/szkoleniowego)

1.19.67 System POWINIEN oferować funkcjonalność klasyfikacji informacji w sposób automatyczny na podstawie przygotowanych polityk lub co najmniej ręcznie przez operatorów Systemu.