

## Wymagania Cyberbezpieczeństwa dla Wykonawcy

Wykonawca zobowiązany jest do spełnienia następujących wymagań:

1. Bezpieczeństwo transmisji danych:
  - Szyfrowanie transmisji danych (np. TLS 1.2+, HTTPS, AES-256) – *KCST-50, KCST-52*.
2. Uwierzytelnianie:
  - Uwierzytelnianie wieloskładnikowe (MFA) dla zdalnego dostępu, usług chmurowych i kont uprzywilejowanych – *KCST-4, KCST-5, KCST-35, KCST-42*.
3. Zarządzanie dostępem:
  - Indywidualne konta użytkowników – *KCST-30*.
  - Weryfikacja dostępów co 6 miesięcy – *KCST-31*.
  - Monitorowanie kont uprzywilejowanych – *KCST-32, KCST-81*.
4. Zabezpieczenia systemowe:
  - Zapory sieciowe – *KCST-20, KCST-74*.
  - Ochrona przed DDoS – *KCST-90*.
  - Web Application Firewall – *KCST-77*.
  - Skanowanie podatności – *KCST-83*.
5. Zarządzanie incydentami:
  - Procedury reagowania – *KCST-86–88*.
  - Zgłaszanie incydentów w ciągu 24h – *KCST-21*.
  - Raportowanie działań naprawczych co 24h.
6. Ochrona danych:
  - Separacja danych ZMPG S.A. – *KCST-36*.
  - Szyfrowanie dokumentów – *KCST-56*.
  - Usuwanie danych zgodnie z NIST 800-88 – *KCST-19, KCST-64*.
7. Szkolenia i świadomość:
  - Coroczne szkolenia z cyberbezpieczeństwa dla użytkowników – *KCST-7*.

Skróty powyżej zapisane kursywą wg. schematu „*KSCT-nr*”, odnoszą się do wymagań, z którymi zgodność winien wykazywać system informatyczny oferowany przez Wykonawcę. Ich wyjaśnienie dostępne jest w dokumencie poniżej pn. „*Wymagania Cyberbezpieczeństwa dla Strony Trzeciej*”.

## Wymagania Cyberbezpieczeństwa dla Strony Trzeciej

### I. Instrukcje reagowania na incydenty cybernetyczne

#### 1. Powiadomienie ZMPG S.A. o incydencie:

- a. Strona Trzecia musi posiadać zdolności do powiadamiania bez zbędnej zwłoki o zaistniałym incydencie Cyberbezpieczeństwa w systemie telefonicznym oraz elektronicznym (zabezpieczona korespondencja e- mail).
- b. Strona Trzecia otrzyma dane kontaktowe oraz szczegóły powiadamiana ZMPG S.A. w momencie zawierania przedmiotu Umowy.

#### 2. Definicje używane przez ZMPG S.A.:

- a. "Aktywa ZMPG S.A. (lub jej Podmiotów Stowarzyszonych)": oznaczają wszystko, co ma wartość dla ZMPG S.A. i jej Podmiotów Stowarzyszonych. stworzone (dane intelektualne i osobowe) lub pozyskane dane, proponowane lub wykonane umowy, umowy, urządzenia, systemy, sprzęt, oprogramowanie, informacje badawcze, podręczniki szkoleniowe, procedury operacyjne lub wsparcia , plany ciągłości działania i wszelkie udogodnienia, które umożliwiają organizacji osiągnięcie celów biznesowych.
- b. "Podejrzane działanie": oznacza każde zaobserwowane zachowanie użytkownika, systemu lub ruchu sieciowego, które może wskazywać lub prowadzić do cyberataku na Aktywa ZMPG S.A. (lub jej Podmiotów Stowarzyszonych), które są wykorzystywane do odbierania, dostępu, przechowywania, przetwarzania lub przesyłania danych.
- c. "Incydent": oznacza faktyczne lub potencjalne prawdopodobieństwo zdarzenia, które zagraża poufności, integralności lub dostępności Aktywów ZMPG S.A. (lub jej Podmiotów Stowarzyszonych) lub zdarzenie, które stanowi naruszenie, lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa, lub zasad dopuszczalnego użytkowania. Rodzaje incydentów:
  - i. Incydent krytyczny - incydent, skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi,
  - ii. Incydent poważny - incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości działania świadczonej usługi kluczowej,
  - iii. Incydent istotny - incydent, który ma istotny wpływ na świadczenie usługi cyfrowej,
  - iv. Incydent o podmiocie publicznym - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny,
  - v. Incydent zwykły - zdarzenie, które ma lub może mieć niekorzystny wpływ na Cyberbezpieczeństwo.

Dodatkowo Incydenty fizyczne obejmują m.in:

- i. Nieautoryzowany fizyczny dostęp do obszarów o ograniczonym dostępie lub pomieszczeń komunikacyjnych,
- ii. Kradzież aktywów ZMPG S.A. (lub jej podmiotów stowarzyszonych),
- iii. Klęski żywiołowe mające wpływ na aktywa ZMPG S.A. (lub jej podmiotów stowarzyszonych).

#### 3. Raportowanie:

- a. Strona Trzecia musi posiadać zdolność do raportowania do ZMPG S.A. z zaistniałego we własnej infrastrukturze incydentu Cyberbezpieczeństwa.
  - b. Strona Trzecia musi przekazać do ZMPG S.A. swoje bieżące działania mające na celu złagodzenie i rozwiązanie Incydentu co dwadzieścia cztery (24) godziny do czasu rozwiązania Incydentu.
  - c. Szczegółowe informacje na temat raportowania ZMPG S.A. przekaże do Strony Trzeciej w momencie zawierania przedmiotu Umowy.
4. Trwałość informacyjna:

Strona Trzecia musi przechowywać obrazy wszystkich znanych systemów informatycznych, których dotyczy Incydent Cyberbezpieczeństwa, przez co najmniej dziewięćdziesiąt (90) dni od złożenia raportu końcowego.

## II. Kontrole Cyberbezpieczeństwa Strony Trzeciej (KCST):

Strona Trzecia musi bezwzględnie spełniać n/w wymagania w zakresie świadczonych przez siebie usług objętych postępowaniem:

1. KCST-1 - Strona Trzecia musi ustanowić, utrzymywać i komunikować Zasady Dopuszczalnego Użytkowania w zakresie Cyberbezpieczeństwa (ZDU) regulujące korzystanie z Zasobów Technologicznych Strony Trzeciej.
2. KCST-2 - Środki ochrony hasłem muszą być egzekwowane przez Stronę Trzecią. Poniżej podano zalecane parametry hasła:
  - a. Minimalna długość: 12 znaków alfanumerycznych i znaków specjalnych.
  - b. Historia: 12 ostatnich haseł.
  - c. Maksymalny wiek: 90 dni na uwierzytelnienie logowania.
  - d. Blokada konta: 5 nieprawidłowych prób logowania.
  - e. Ustawienia wygaszacza ekranu: automatyczne blokowanie po 15 minutach bezczynności,
  - f. Bezwzględne wylogowywanie się użytkownika z konta w momencie zakończenia/przerwy w pracy na stacji roboczej.
3. KCST-3 - Podmiotom zewnętrznym nie wolno zapisywać, przechowywać elektronicznie w postaci niezaszyfrowanej ani ujawniać żadnych haseł ani kodów uwierzytelniających, które są używane do uzyskiwania dostępu do Aktywów lub Obiektów krytycznych. Powinno to być częścią Polityki/Standardu Cyberbezpieczeństwa Strony Trzeciej.
4. KCST-4 - Uwierzytelnianie wieloskładnikowe musi być egzekwowane w przypadku każdego zdalnego dostępu, w tym dostępu z Internetu, do zasobów komputerowych firmy zewnętrznej.
5. KCST-5 - Uwierzytelnianie wieloskładnikowe musi być egzekwowane we wszystkich usługach w chmurze wykorzystywanych przez Stronę Trzecią, w tym w dostępie do poczty e-mail opartej na chmurze.
6. KCST-6 - Strona Trzecia musi poinformować ZMPG S.A., gdy pracownicy, którym udostępniono dane uwierzytelniające użytkownika ZMPG S.A., nie potrzebują już dostępu, zostali przeniesieni, ponownie przydzieleni, przeszli na emeryturę, zrezygnowali lub nie są już związani ze Stroną Trzecią.
7. KCST-7 - Strona Trzecia musi wymagać, aby wszyscy użytkownicy systemów informatycznych brali udział w corocznym obowiązkowym szkoleniu cyberbezpieczeństwa, które dotyczy dopuszczalnego użytkowania i dobrych praktyk informatycznych. Szkolenie musi obejmować następujące tematy:

- a. Bezpieczeństwo w Internecie i mediach społecznościowych
  - b. Zasady Dopuszczalnego Użytkowania (ZDU)
  - c. Inżynieria społeczna i wiadomości phishingowe
  - d. Udostępnianie danych uwierzytniających (tj. nazwy użytkownika i hasła)
  - e. Bezpieczeństwo danych.
8. KCST-8 - Strona Trzecia musi poinformować personel, zgodnie z polityką firmy Strony Trzeciej, że używanie osobistej poczty elektronicznej do udostępniania i przesyłania danych ZMPG S.A. jest surowo zabronione.
  9. KCST-9 - Strona Trzecia musi poinformować personel, zgodnie z polityką firmy Strony Trzeciej, że ujawnianie polityk, procedur i standardów ZMPG S.A. lub wszelkiego rodzaju danych nieupoważnionym podmiotom lub w Internecie jest surowo zabronione.
  10. KCST-10 - Wszystkie aktywa i systemy technologiczne Strony Trzeciej muszą być chronione hasłem.
  11. KCST-11 - Aktywa i systemy technologiczne Stron Trzecich muszą być regularnie aktualizowane: system operacyjny (OS), oprogramowanie i poprawki apletów (tj. Adobe, Flash, Java itp.).
  12. KCST-12 - Zasoby technologiczne Stron Trzecich muszą być chronione oprogramowaniem antywirusowym (AV). Aktualizacje muszą być stosowane codziennie, a pełne skanowanie systemu musi być wykonywane co najmniej co dwa tygodnie.
  13. KCST-13 - Strona Trzecia musi wdrożyć technologię Sender Policy Framework (SPF) na serwerze poczty.
  14. KCST-14 - Strona Trzecia musi egzekwować funkcję Sender Policy Framework (SPF) w domenach e-mail ZMPG S.A.: @portgdansk.pl
  15. KCST-15 - Strona Trzecia musi opublikować rekord SPF na serwerze DNS.
  16. KCST-16 - Strona Trzecia musi sprawdzać wszystkie przychodzące wiadomości e-mail pochodzące z Internetu przy użyciu ochrony antyspamowej.
  17. KCST-17 - Strona Trzecia musi korzystać z prywatnej domeny e-mail. Domeny ogólne, takie jak Gmail i Hotmail, nie mogą być używane.
  18. KCST-18 - Strona Trzecia musi dysponować formalnymi procedurami dotyczącymi zwalniania pracowników. Procedury off-boardingu muszą obejmować zwrot aktywów i usunięcie wszystkich powiązanych dostępów.
  19. KCST-19 - Aktywa wykorzystywane do przetwarzania lub przechowywania danych i informacji ZMPG S.A. muszą zostać usunięte / wyczyszczone przed końcem Cyklu życia danych lub przed końcem okresu przechowywania, jak określono w Umowie, jeśli został on zdefiniowany. Obejmuje to wszystkie kopie danych, takie jak kopie zapasowe utworzone u Strony Trzeciej. Usuwanie / czyszczenie musi być przeprowadzone zgodnie ze Standardem NIST 800-88 z uwzględnieniem wymagań Ustawy o Ochronie Danych Osobowych. Strona Trzecia musi oświadczyć ZMPG S.A. na piśmie, że proces usuwania / czyszczenia danych został zakończony.
  20. KCST-20 - Zapory sieciowe muszą być skonfigurowane i włączone na urządzeniach końcowych.
  21. KCST-21 - Strona Trzecia po wykryciu Incydentu Cyberbezpieczeństwa oprócz reagowania wg swoich przyjętych procedur/polityk/standardów w celu rozwiązania i złagodzenia Incydentu musi:

- a. Powiadomić ZMPG S.A. w ciągu dwudziestu czterech (24) godzin od wykrycia Incydentu,
  - b. Należy postępować zgodnie z instrukcjami powiadamiania i raportowania na Incydenty Cybernetyczne w ZMPG S.A.
22. KCST-22 - Strona Trzecia musi posiadać zasady i procesy, aby klasyfikować informacje pod względem ich wartości, krytyczności i poufności.
  23. KCST-23 - Strona Trzecia musi ustanowić, utrzymywać i informować o Politykach i Standardach Cyberbezpieczeństwa.
  24. KCST-24 - Strona Trzecia musi zatrudniać pracowników, których głównym obowiązkiem jest cyberbezpieczeństwo. Obowiązki tego personelu muszą obejmować utrzymanie bezpieczeństwa systemów informatycznych i zapewnienie zgodności z istniejącymi politykami.
  25. KCST-25 - Strona Trzecia musi przeprowadzać coroczne zewnętrzne testy penetracyjne w swoich systemach infrastruktury IT i aplikacjach internetowych.
  26. KCST-26 - Strona Trzecia musi przeprowadzać coroczne zewnętrzne testy penetracyjne na usługach Cloud Computing używanych przez ZMPG S.A.
  27. KCST-27 - Strona Trzecia hostująca stronę internetową dla ZMPG S.A., musi przeprowadzać coroczne testy penetracyjne w celu sprawdzenia bezpieczeństwa strony internetowej.
  28. KCST-28 - Zewnętrzne centrum danych (Data Center) musi spełniać wymagania krajowe i UE.
  29. KCST-29 - Strona Trzecia musi posiadać proces regularnego przeprowadzania Oceny Ryzyka Cyberbezpieczeństwa, aby identyfikować, oceniać i eliminować Ryzyka dla danych i systemów informatycznych.
  30. KCST-30 - Użytkownicy uzyskujący dostęp do aplikacji i systemów informatycznych muszą otrzymać unikalne (indywidualne) loginy i hasła. Konta ogólne nie mogą być dozwolone, chyba że wyraźnie zatwierdzone, ograniczone i kontrolowane.
  31. KCST-31 - Dostęp użytkownika do systemu operacyjnego, aplikacji i bazy danych musi być sprawdzany co pół roku w celu ustalenia, czy personel nadal wymaga takiego dostępu.
  32. KCST-32 - Wszystkie konta uprzywilejowane muszą być ograniczone, uzasadnione i regularnie sprawdzane.
  33. KCST-33 - Zdalny dostęp administracyjny z Internetu nie może być dozwolony, chyba że zostanie wyraźnie zatwierdzony, ograniczony i kontrolowany.
  34. KCST-34 - Połączenia sieciowe z systemami informatycznymi i aplikacjami w lokalizacji Stron Trzecich muszą być autoryzowane i monitorowane.
  35. KCST-35 - Uwierzytelnianie wieloskładnikowe musi być wymuszane na wszystkich uprzywilejowanych kontach , w tym na zdalnym dostępie do systemów informatycznych i aplikacji.
  36. KCST-36 - Strona trzecia musi logicznie (np. partycjonując dysk fizyczny ) i/lub fizycznie oddzielić dane, które są związane z ZMPG S.A. od danych innych kontrahentów.
  37. KCST-37 - Dane krytyczne ZMPG S.A. mogą być udostępniane wyłącznie ograniczonej liczbie osób, które biorą udział w części pracach określonych w Umowie.
  38. KCST-38 - Podsieci serwerów i stacji roboczych muszą być podzielone na segmenty, a dostęp między nimi jest ograniczony i monitorowany.
  39. KCST-39 - Serwery dostępne z Internetu muszą być umieszczone w DMZ (tj. sieci obwodowej) z ograniczonym dostępem do wewnętrznych podsieci.

40. KCST-40 - Sieci bezprzewodowe uzyskujące dostęp do systemów informatycznych muszą wykorzystywać silne szyfrowanie do uwierzytelniania i transmisji, takie jak WPA2 lub WPA2 Enterprise.
41. KCST-41 - Centrum danych Strony Trzeciej musi posiadać wymaganą ocenę poziomu i wysoką dostępność przełączania awaryjnego usług zgodnie z wymaganiami ZMPG S.A.
42. KCST-42 - Uwierzytelnianie wieloskładnikowe musi być wymuszane na Użytkownikach ZMPG S.A. uzyskujących dostęp do usługi chmury obliczeniowej dostawcy usług w chmurze przechowującej lub hostującej krytyczne dane ZMPG S.A.
43. KCST-43 - Uwierzytelnianie wieloskładnikowe musi być wymuszane na użytkownikach końcowych uzyskujących dostęp do systemu zarządzania treścią (CMS).
44. KCST-44 - Wszystkie systemy (routery, przełączniki, serwery i zapory ogniowe) muszą być umieszczone w pomieszczeniu komunikacyjnym i w zamkniętej szafie dystrybucyjnej. Dostęp do pomieszczenia komunikacyjnego musi być uzależniony od wymogów bezpieczeństwa, takich jak czytniki kart dostępu lub urządzenia biometryczne.
45. KCST-45 - Strona Trzecia musi definiować proces zarządzania osobami odwiedzającymi Stronę Trzecią. Proces ten powinien obejmować prowadzenie i regularne przeglądanie dzienników gości. Dziennik odwiedzin powinien zawierać takie informacje jak:
  - a. Identyfikator odwiedzającego
  - b. Cel wizyty
  - c. Data i godzina wejścia/wyjścia.
46. KCST-46 - Osoby odwiedzające obiekty o znaczeniu krytycznym Strony Trzeciej muszą być zawsze eskortowane przez osoby upoważnione.
47. KCST-47 - Strona Trzecia musi wyznaczyć obszar roboczy z ograniczonym dostępem dla personelu mającego dostęp do sieci/danych ZMPG S.A.
48. KCST-48 – Nośniki kopii zapasowych muszą być zabezpieczone w celu zablokowania/unieemożliwienia nieautoryzowanego dostępu fizycznego.
49. KCST-49 - Zasoby technologiczne i systemy podłączone do Internetu muszą być licencjonowane i obsługiwane przez dostawcę.
50. KCST-50 - Strona Trzecia musi szyfrować przesyłane dane (np. SSH, FTPS, HTTPS, TLS, IPSEC).
51. CST-51 - Strona Trzecia musi szyfrować (np. za pomocą HTTPS) sesje, w których krytyczne informacje lub dane ZMPG S.A. będą przesyłane z i do usługi przetwarzania w chmurze publicznej i wymuszać uwierzytelnianie, blokadę i limit czasu sesji.
52. KCST-52 - Strona Trzecia musi wdrożyć mechanizmy szyfrowania, przy użyciu co najmniej algorytmu szyfrowania AES i 256 bitów.
53. KCST-53 – Zdolność zarządzania kluczami szyfrującymi, w tym przechowywanie i odzyskiwanie, musi być zdefiniowana, stosowana, i okresowo weryfikowana.
54. KCST-54 - Strona Trzecia musi wdrożyć mechanizm kontroli urządzenia na Aktywach, które są wykorzystywane do odbierania, przechowywania, przetwarzania lub przesyłania danych ZMPG S.A., takich jak wyłączanie korzystania z zewnętrznych nośników pamięci.
55. KCST-55 - Dostęp do Internetu musi być ograniczony za pomocą technologii filtrowania treści w celu ograniczenia dostępu do poczty elektronicznej, usług przechowywania w chmurze oraz blokowania złośliwych lub niepożądanych stron internetowych.

56. KCST-56 - Dokumenty zawierające dane krytyczne ZMPG S.A. muszą być szyfrowane i bezpiecznie przechowywane, a dostęp do nich musi być ograniczony do upoważnionego personelu.
57. KCST-57 - Rozwiązanie zdalnego czyszczenia musi być zainstalowane na wszystkich tabletach i telefonach komórkowych używanych do odbierania, przechowywania i/lub produkcji krytycznych danych dla ZMPG S.A.
58. KCST-58 – Strona Trzecia musi wdrożyć walidację danych we wszystkich polach wejściowych dla aplikacji lub usług przetwarzania w chmurze używanych przez ZMPG S.A., aby akceptować tylko dane wejściowe z prawidłowym typem danych, składnią i zakresem długości.
59. KCST-59 – Komunikaty o błędach aplikacji nie mogą wyświetlać żadnych poufnych informacji. Objaśnienie: Niewłaściwa obsługa błędów może wprowadzić wiele problemów związanych z bezpieczeństwem strony internetowej. Najczęstszym problemem jest wyświetlanie użytkownikowi (hakerowi) szczegółowych wewnętrznych komunikatów o błędach, takich jak ślady stosu, zrzuty bazy danych i kody błędów. Komunikaty te ujawniają szczegóły implementacji, które nigdy nie powinny zostać ujawnione. Takie szczegóły mogą dostarczyć hakerom ważnych wskazówek na temat potencjalnych błędów w witrynie, a takie komunikaty są również niepokojące dla zwykłych użytkowników.
60. KCST-60 – Aplikacja nie może przechowywać, generować, przysyłać ani używać haseł w postaci zwykłego tekstu.
61. KCST-61 - Strona Trzecia musi utworzyć i zarządzać podstawowymi konfiguracjami w celu wzmocnienia systemów informatycznych. Proces wzmocniania musi dotyczyć konfiguracji takich jak: - Resetowanie domyślnych nazw użytkownika/hasła, - Wyłączanie niepotrzebnego oprogramowania, - Wyłączanie niepotrzebnych usług.
62. KCST-62 - Strona Trzecia musi ustanowić i przestrzegać regularnych procedur dotyczących tworzenia kopii zapasowych krytycznych systemów oraz danych, oprogramowania i stron internetowych ZMPG S.A.
63. KCST-63 - Kopie zapasowe przechowywane w lokalizacji zewnętrznej muszą być zaszyfrowane przy użyciu co najmniej algorytmu szyfrowania AES, i 256-bitowego klucza, z wyjątkiem danych sklasyfikowanych jako publiczne.
64. KCST-64 - Strona Trzecia musi wdrożyć proces sanityzacji (czyszczenia i usuwania danych) zanim jakiegokolwiek Aktywa zostaną przekazane, zniszczone, przeniesione lub uzupełnione. Proces ten musi być dostosowany do najlepszych praktyk branżowych, takich jak NIST 800 - 88.
65. KCST-65 - Strona Trzecia musi posiadać Plan Odtwarzania po Awarii / Odtwarzanie Awaryjne (DRP), który jest udokumentowany, utrzymywany i przekazywany odpowiednim Stronom. Plan Odtwarzania po Awarii powinien dotyczyć odtworzenia Aktywów i komunikacji po poważnym zakłóceniu działalności biznesowej.
66. KCST-66 - Strona Trzecia musi posiadać kompleksowy Plan Ciągłości Działania (BCP), który jest udokumentowany, utrzymywany i przekazywany odpowiednim stronom. BCP powinien uwzględniać wystąpienie następujących scenariuszy:
  - a. Awaria sprzętu,
  - b. Zakłócenie zasilania lub komunikacji,
  - c. Awaria aplikacji lub uszkodzenie bazy danych,
  - d. Błąd ludzki, sabotaż lub strajk,
  - e. Atak złośliwego oprogramowania,

- f. Hakowanie lub inne ataki internetowe,
  - g. Niepokoje społeczne lub ataki terrorystyczne,
  - h. Katastrofy ekologiczne,
  - i. Dane kontaktowe personelu przeznaczonego do reagowania w nagłych wypadkach.
67. KCST-67 - Strona Trzecia musi zapewnić, że właściciele Planu Ciągłości Działania (BCP) są zidentyfikowani, a BCP jest corocznie przeglądany i aktualizowany.
68. KCST-68 - Strona Trzecia musi przeprowadzać ćwiczenia ciągłości działania co najmniej raz w roku.
69. KCST-69 - Strona Trzecia musi posiadać formalne procedury dotyczące zatrudniania pracowników uzyskujących uprzywilejowany dostęp do danych, które powinny dawać rękojmię bezpieczeństwa przetwarzanych informacji/danych.
70. KCST-70 - Strona Trzecia musi przeprowadzić skanowanie bezpieczeństwa wszystkich opracowanych aplikacji i usunąć wszystkie wykryte luki w zabezpieczeniach przed ich wdrożeniem w środowisku produkcyjnym.
71. KCST-71 - Wszystkie zmiany w aplikacji muszą być odpowiednio autoryzowane i przetestowane w środowisku testowym przed wdrożeniem w środowisko produkcyjne.
72. KCST-72 - Strona Trzecia musi mieć proces bezpiecznego systemu i cyklu życia rozwoju oprogramowania zgodny z najlepszymi praktykami branżowymi.
73. KCST-73 - Strona Trzecia musi przechowywać wszystkie dzienniki audytu z systemów informatycznych i aplikacji przechowujących, przetwarzających lub przesyłających dane ZMPG S.A. przez jeden (1) rok.
74. KCST-74 - Zapory sieciowe muszą być zaimplementowane w sieci obwodowej i tylko wymagane usługi mogą być dozwolone. Podatne usługi lub niezabezpieczone protokoły powinny zostać zablokowane.
75. KCST-75 - Systemy wykrywania włamań (IDS) lub systemy zapobiegania włamaniom (IPS) muszą być wdrożone na obwodzie sieci.
76. KCST-76 - Sygnatury firewalli, IDS i IPS muszą być aktualne.
77. KCST-77 - Strona Trzecia hostująca aplikację lub stronę internetową dla ZMPG S.A. musi wdrożyć rozwiązanie typu Web Application Firewall w celu sprawdzania całego ruchu przychodzącego pod kątem potencjalnych zagrożeń i złośliwej aktywności, np. wstrzykiwania SQL i Cross Site Scripting.
78. KCST-78 - Strona Trzecia musi monitorować Aktywa Technologiczne, Systemy i aplikacje w celu identyfikacji nieautoryzowanego dostępu lub nieautoryzowanych działań.
79. KCST-79 - Strona Trzecia musi okresowo agregować i korelować dane z wielu systemów i krytycznych aplikacji, takich jak zapory ogniowe, IDS/IPS i antywirusy, w centralnym repozytorium w celu monitorowania i analizy zdarzeń.
80. KCST-80 - Należy wdrożyć wiele środków bezpieczeństwa fizycznego, aby zapobiec nieautoryzowanemu dostępowi do obiektów. Wejścia i wyjścia muszą być zabezpieczone za pomocą klucza karty uwierzytelniającej, zamków do drzwi i monitorowane przez kamery wideo (CCTV).
81. KCST-81 - Aktywność kont uprzywilejowanych musi być rejestrowana i regularnie monitorowana.

82. KCST-82 - Nieautoryzowane urządzenia (takie jak urządzenia osobiste i telefony komórkowe) nie mogą być używane do przechowywania, przetwarzania lub dostępu do Zasobów.
83. KCST-83 - Comiesięczne skanowanie pod kątem luk w zabezpieczeniach musi być przeprowadzane w celu oceny konfiguracji, poprawek i usług pod kątem znanych luk w zabezpieczeniach.
84. KCST-84 - Fizyczny dostęp do obiektu, w którym znajdują się systemy informatyczne, musi być ograniczony do upoważnionego personelu i regularnie sprawdzany.
85. KCST-85 - Systemy informatyczne i aplikacje muszą rejestrować zdarzenia podlegające audytowi, takie jak uruchomienie systemu, zamknięcie systemu, ponowne uruchomienie nieudane próby logowania, utworzenie usługi, dodanie konta użytkownika, usunięcie konta użytkownika itp.
86. KCST-86 - Polityka i plan zarządzania incydentami muszą być udokumentowane, utrzymywane i przekazywane kierownictwu i odpowiednim członkom zespołu/działu.
87. KCST-87 - Strona Trzecia musi posiadać zdolność reagowania na incydenty, która obejmuje przygotowanie, wykrywanie i analizę, powstrzymywanie, eliminację, odzyskiwanie, dokumentację i zabezpieczenie dowodów, protokoły komunikacji i wyciągnięte wnioski.
88. KCST-88 - Strona Trzecia musi śledzić, klasyfikować i dokumentować wszystkie Incydenty Cyberbezpieczeństwa.
89. KCST-89 - Strona Trzecia musi rozwiązywać lub mitygować zidentyfikowane luki w zabezpieczeniach w systemie, komputerze, sieci lub innym sprzęcie komputerowym w następujących ramach czasowych:
  - a. Ryzyko krytyczne: natychmiastowy patch do czternastu (14) dni kalendarzowych od wydania krytycznej poprawki przez dostawcę, powiadomienia od ZMPG S.A. lub wykrycia naruszenia bezpieczeństwa w zależności od tego, co nastąpi wcześniej.
  - b. Wysokie ryzyko: w ciągu jednego (1) miesiąca od wydania przez dostawcę poprawki lub wykrycia naruszenia bezpieczeństwa, w zależności od tego, co nastąpi wcześniej.
  - c. Średnie i niskie ryzyko: w ciągu trzech (3) miesięcy od wykrycia.
90. KCST-90 - Jeśli Strona Trzecia hostuje witrynę internetową lub świadczy Usługi w Chmurze dla ZMPG S.A, witryna internetowa lub Usługi w Chmurze muszą być zabezpieczone za pomocą ochrony przed rozproszonymi atakami typu DDOS (Distributed Denial of Service).