

System OT PSG może być wykorzystywany przez Użytkowników OT wyłącznie zgodnie z zapisami określonymi w Zasadach.

Niniejszy dokument zawiera uszczegółowienie zasad bezpieczeństwa dla Systemu OT, których spełnienie zapewnia:

- właściwy poziom bezpieczeństwa teleinformatycznego Systemu OT w PSG (zapewnienie Poufności, Dostępności, Integralności i Rozliczalności);
- efektywne kosztowo zarządzanie ryzykiem bezpieczeństwa informacji;
- zgodność podejmowanych działań w obszarze ochrony Systemu OT z regulacjami prawnymi obowiązującymi na terenie Rzeczypospolitej Polskiej.

Niestosowanie się do powyższych zasad może skutkować, co najmniej ograniczeniem lub odebraniem uprawnień do korzystania z Systemu OT.

1. Role i odpowiedzialności

- 1.1.1. Biuro Bezpieczeństwa Teleinformatycznego odpowiada za określanie wytycznych w zakresie zarządzania bezpieczeństwem Systemu OT w PSG.
- 1.1.2. Departament Teleinformatyki i Cyberbezpieczeństwa odpowiada za dostarczanie Użytkownikom OT środowiska teleinformatycznego dla Systemu OT (tj. sieci komputerowej, infrastruktury serwerowej, sprzętu komputerowego), zapewnienie dostępu (w tym zarządzanie uprawnieniami) do tego środowiska oraz za dostarczanie Systemów informatycznych OT i administrowanie nimi.
- 1.1.3. Obszar OT odpowiada za architekturę i utrzymanie Systemu OT (z wyłączeniem Systemów Informatycznych OT), dostarczanie i eksploatację Urządzeń OT, zarządzanie zmianą w Systemie OT (z wyłączeniem Systemów Informatycznych OT) oraz za prawidłową i efektywną realizację realizowanych procesów.

2. Bezpieczeństwo Systemu OT

2.1. System OT – podstawowe zasady bezpieczeństwa

- 2.1.1. W PSG wprowadza się separację środowiska Systemu OT od środowiska IT. Separacja środowiska Systemu OT musi zapewnić jego ochronę przed wyciekami informacji, cyberzagrożeniami i nieautoryzowanym dostępem.
- 2.1.2. Architektura środowiska Systemu OT w PSG musi zapewnić jego skuteczną izolację od środowiska IT.
- 2.1.3. Na potrzeby Systemu OT utworzono w PSG dedykowaną Domenę OT. Pomędzy Domeną OT a Domeną PSG nie ma ustanowionych żadnych relacji zaufania.
- 2.1.4. System OT powinien być zainstalowany i użytkowany w Domenie OT.
- 2.1.5. W uzasadnionych przypadkach (np. wysoki koszt migracji, systemy wygaszane) dopuszcza się użytkowanie Systemów informatycznych OT w Domenie PSG.

- 2.1.6. Wdrożenia Systemów informatycznych OT oraz wprowadzane w nich zmiany muszą być uzgadniane z Departamentem Teleinformatyki i Cyberbezpieczeństwa.
- 2.1.7. Komunikacja z Systemem OT musi być ograniczona i zabezpieczona.
- 2.1.8. W Systemie OT należy dokonać kategoryzacji Obiektów OT pod kątem ważności w kontekście bezpieczeństwa teleinformatycznego oraz określić wymagania bezpieczeństwa teleinformatycznego dla poszczególnych kategorii Obiektów OT. Wyniki przeprowadzonej kategoryzacji Obiektów OT zawiera Załącznik nr 1 do niniejszego załącznika.
- 2.1.9. W odniesieniu do każdego z Obiektów OT typu stacja gazowa musi być opracowana i aktualizowana karta stacji gazowej zawierająca dane identyfikacyjne i technologiczne, schemat stacji, poglądowe zdjęcie oraz wynik szacowania ryzyka bezpieczeństwa sieci dystrybucyjnej przy naruszeniu zabezpieczeń teleinformatycznych zgodnie z „Procedurą zarządzania ryzykiem w PSG”. Szablon karty stacji gazowej zawiera Załącznik nr 2 do niniejszego załącznika.
- 2.1.10. Dla każdego Obiektu OT typu stacja gazowa powinien zostać zastosowany odpowiedni standard (wariant) budowy Sieci OT określony na podstawie ustanowionej metodyki. Dopuszcza się wykorzystanie standardu (wariantu) wyższego. Metodyka doboru topologii oraz standardy (warianty) Sieci OT dla Obiektów OT typu stacja gazowa opisane są w Załączniku nr 3 do niniejszego załącznika.

2.2. Dostęp Użytkowników do Systemu OT

- 2.2.1. Podstawowe założenie dotyczące zarządzania dostępem Użytkowników OT zakłada, że wszelki dostęp do zasobów Systemu OT jest zabroniony z wyjątkiem tego, który został wyraźnie określony jako dozwolony.
- 2.2.2. Wnioskowanie, dokumentowanie procesu akceptacji i ewidencjonowanie uprawnień dla zasobów Systemu OT odbywa się w istniejącej instancji systemu do wnioskowania o uprawnienia do Systemów informatycznych i procesu akceptacyjnego z zachowaniem zasad stosowanych dla Użytkowników zakładanych na podstawie kont AD w Domenie PSG.
- 2.2.3. Dane uwierzytelniające Użytkowników OT muszą być chronione przed nieautoryzowanym dostępem zarówno po stronie Użytkowników OT, jak i po stronie Systemu OT.
- 2.2.4. Dostęp do Systemu OT mogą posiadać tylko Użytkownicy OT.
- 2.2.5. Użytkownik OT może się logować jedynie do tych zasobów Systemu OT, które są niezbędne do wykonywania obowiązków służbowych.
- 2.2.6. W Domenie OT Użytkownicy OT mogą posiadać tylko jedno konto. Wyjątek stanowią konta serwisowe wyznaczonych Pracowników IT lub Inżynierów OT.
- 2.2.7. Wykorzystywanie kont serwisowych w Systemach informatycznych OT i Urządzeniach OT jest dozwolone wyłącznie, gdy uzasadniają to ważne potrzeby biznesowe i nie ma innego sposobu zapewnienia dostępu do Systemu OT.

- 2.2.8. Użytkownik OT nie może posiadać uprawnień administratora lub innych uprawnień umożliwiających instalację/odinstalowywanie oprogramowania, lub dokonywanie zmian konfiguracyjnych w Systemach informatycznych OT lub Urządzeniach OT.
- 2.2.9. Za administrowanie i zarządzanie dostępem do Urządzeń OT odpowiadają Inżynierowie OT.
- 2.2.10. Wszystkie konta administracyjne w Systemach informatycznych OT i w Urządzeniach OT muszą być identyfikowalne.
- 2.2.11. Podczas wykonywania czynności w Systemach informatycznych OT lub Urządzeniach OT niewymagających użycia kont administracyjnych zabrania się ich stosowania.
- 2.2.12. Bezpośredni dostęp do konsoli serwerów Systemów informatycznych OT (z wykorzystaniem kont administracyjnych) lub Urządzeń OT jest dozwolony tylko dla Inżynierów OT. Inny Użytkownik OT może uzyskać taki dostęp za akceptacją Inżyniera OT.
- 2.2.13. Dostęp Użytkowników OT do zasobów Systemu OT musi być realizowany z wykorzystaniem Terminali PAW. Dotyczy to zarówno dostępu z sieci komputerowej PSG jak i dostępu zdalnego z zastosowaniem VPN. Terminale PAW nie mogą mieć dostępu do Internetu.

2.3. Dostęp Podmiotów zewnętrznych do Systemu OT

- 2.3.1. Dostęp Podmiotów zewnętrznych do środowisk produkcyjnych Systemów informatycznych OT jest zabroniony.
- 2.3.2. Podmioty zewnętrzne mogą uzyskać dostęp tylko do środowisk testowych lub deweloperskich Systemów informatycznych OT (w sieci komputerowej PSG) na podstawie zawartej umowy z PSG, w której zostaną określone zasady dostępu, zakres i okres dostępu oraz niezbędne wymagania bezpieczeństwa teleinformatycznego.
- 2.3.3. Nawiązanie połączenia zdalnego z Systemami informatycznymi OT może być realizowane wyłącznie za pośrednictwem tzw. serwera przesiadkowego, odpowiednio skonfigurowanego i zarządzanego, pełniącego rolę pośredniego punktu uwierzytelnienia w sieci komputerowej PSG.
- 2.3.4. Pracownicy Podmiotów zewnętrznych mogą przebywać w pomieszczeniach, w których znajdują się zasoby Systemu OT (w tym w Obiektach OT) jedynie pod nadzorem pracownika PSG.
- 2.3.5. Konta dostępowe Podmiotów zewnętrznych do poszczególnych Systemów informatycznych OT i Urządzeń OT powinny być odblokowywane przez Inżyniera OT tylko na czas bezpośredniego wykonywania w nich prac.
- 2.3.6. Pracownicy Podmiotów zewnętrznych mogą logować się do konsoli Urządzeń OT w Obiektach OT tylko lokalnie (bez dostępu zdalnego) i w obecności Inżyniera OT.
- 2.3.7. Dostęp Podmiotów zewnętrznych do Systemu OT musi być przeanalizowany pod kątem bezpieczeństwa. Korzyści związane z dostępem Podmiotów zewnętrznych muszą uwzględniać ryzyka związane z takim dostępem.

2.4. Standaryzacja i zabezpieczenia zasobów Systemu OT

- 2.4.1. W Systemie OT powinny być ustanowione standardy techniczne w zakresie wykorzystywanych w Obiektach OT Urządzeń komunikacyjnych OT, zapewniające bezpieczeństwo teleinformatyczne. Ustanowione w PSG standardy techniczne dla Urządzeń komunikacyjnych OT zawiera Załącznik nr 4 do niniejszego załącznika.
- 2.4.2. Dla wykorzystywanych w Obiektach OT Urządzeń komunikacyjnych OT powinny być określone i stosowane standardy ich konfiguracji w Systemie OT. Ustanowione w PSG standardy konfiguracji dla Urządzeń komunikacyjnych OT zawiera Załącznik nr 5 do niniejszego załącznika.
- 2.4.3. Nowe lub modernizowane Obiekty OT powinny wykorzystywać tylko Urządzenia komunikacyjne OT zgodne z ustanowionymi standardami.
- 2.4.4. Sterowanie Urządzeniami OT w Systemie OT (w tym z wykorzystaniem Systemów informatycznych OT) musi być nadzorowane i wykonywane przez autoryzowanych do tego Użytkowników OT.
- 2.4.5. Domyślne konta dostępowe do zasobów Systemu OT muszą zostać wyłączone, jeśli jest to technicznie możliwe.
- 2.4.6. Wszystkie domyślne hasła dostępowe do zasobów Systemu OT muszą zostać zmienione.
- 2.4.7. Użytkownik OT nie może logować się do BIOS zasobów Systemu informatycznego OT.
- 2.4.8. W Domenie OT nie ustanowiono Użytkownikom OT dostępu do Internetu oraz Poczty elektronicznej PSG.
- 2.4.9. W Domenie OT nie stosuje się rozwiązań wykorzystujących chmurę publiczną.
- 2.4.10. Bezpośredni dostęp do Systemu OT z Internetu jest zabroniony.
- 2.4.11. Na komputerach przenośnych wykorzystywanych w Systemie OT musi być zablokowana możliwość podłączania się do obcych sieci WiFi.
- 2.4.12. Karty SIM wykorzystywane w Urządzeniach OT muszą pracować w dedykowanym APN prywatnym.
- 2.4.13. Urządzenia OT powinny wykorzystywać bezpieczne protokoły komunikacyjne.
- 2.4.14. Urządzenia OT powinny podlegać regularnej aktualizacji oprogramowania (np. firmware, poprawki bezpieczeństwa). Zastosowanie w środowisku OT urządzeń z zaktualizowanym oprogramowaniem musi być poprzedzone testami urządzeń w celu zapewnienia ciągłości działania środowiska OT.
- 2.4.15. Na potrzeby środowiska OT musi zostać udostępniony dedykowany serwer plików i serwer FTP.

2.5. Monitorowanie i bezpieczeństwo zasobów Systemu OT

- 2.5.1. Wszystkie Systemy informatyczne OT powinny zapewnić możliwość tworzenia i monitorowania dzienników zdarzeń dotyczących systemu operacyjnego w celu umożliwienia rejestracji działań Użytkowników OT na wszystkich zasobach tych systemów.

- 2.5.2. Inżynier OT zobowiązany jest do przeglądania i analizy zapisów w dzienniku zdarzeń danego Systemu informatycznego OT lub logów Urządzenia OT.
- 2.5.3. Dzienniki zdarzeń oraz logi należy zabezpieczyć przed modyfikacją i nieuprawnionym dostępem.
- 2.5.4. Dla Systemów informatycznych OT powinno być prowadzone monitorowanie wydajności, zajętości przestrzeni dyskowej i obciążenia poszczególnych zasobów prowadzone w trybie ciągłym z zapewnieniem odpowiedniej reakcji na ewentualne przyszłe problemy związane z dostępnością zasobów.
- 2.5.5. Systemy informatyczne OT lub Urządzenia OT muszą być objęte systemem monitorowania ruchu sieciowego oraz analizy logów w celu szybkiego wykrywania i reagowania na potencjalne zagrożenia i Awarie IT. Logi bezpieczeństwa muszą być przesyłane do systemu SIEM a zdarzenia bezpieczeństwa monitorowane przez zespół SOC.
- 2.5.6. W odniesieniu do sprzętu komputerowego wykorzystywanego w Systemie OT powinny być wykorzystywane (w konfiguracji on-premise) systemy zarządzania zasobami (np. SCCM, WSUS), rozwiązania EDR oraz zaawansowane narzędzia analityki zagrożeń.
- 2.5.7. W Systemie OT wymaga się regularnego skanowania podatności. Skanowanie może odbywać się z wykorzystaniem tylko takich narzędzi, które odpytują zasoby Systemów informatycznych OT oraz Urządzenia OT w sposób bezpieczny w celu zapewnienia ciągłości ich pracy. Urządzenia OT mogą być skanowane wyłącznie w dedykowanym środowisku laboratoryjnym.
- 2.5.8. Dla Systemów informatycznych OT oraz Urządzeń OT wymaga się przeprowadzania testów bezpieczeństwa, aby ocenić skuteczność zabezpieczeń i zidentyfikować ewentualne słabości. Testy należy przeprowadzać obowiązkowo przed uruchomieniem Systemu informatycznego OT lub zastosowaniem Urządzenia OT, jak również po wprowadzeniu zmian, które mogą mieć wpływ na bezpieczeństwo.
- 2.5.9. Wymaga się regularnego przeprowadzania aktualizacji bezpieczeństwa (udostępnianych przez producentów) dla Systemów informatycznych OT i Urządzeń OT, aby zapobiegać wykorzystaniu luk w zabezpieczeniach. Aktualizacje muszą być przeprowadzane po przetestowaniu z uwzględnieniem ryzyka w zakresie ciągłości działania.

2.6. Sieć OT

- 2.6.1. Na potrzeby Systemu OT musi być wydzielona z sieci komputerowej PSG dedykowana odseparowana Sieć OT.
- 2.6.2. Wymiana informacji pomiędzy Siecią OT, a innymi sieciami możliwa jest tylko poprzez dedykowaną strefę DMZ.
- 2.6.3. Za separację Sieci OT od reszty sieci komputerowej PSG i jej monitorowanie odpowiada Departament Teleinformatyki i Cyberbezpieczeństwa.

- 2.6.4. Wewnętrzna adresacja IP, konfiguracja usług sieciowych, topologia, nazwy i modele urządzeń Sieci OT oraz informacja o zasobach powiązanych nie może być ujawniana osobom nieuprawnionym.
- 2.6.5. Dostęp konfiguracyjny do Urządzeń aktywnych w Sieci OT powinien być ograniczony tylko do autoryzowanych Inżynierów OT.
- 2.6.6. Użytkownikom OT należy zapewnić dostęp tylko do tych usług środowiska Systemu OT, do których posiadają uprawnienia.
- 2.6.7. Niezabezpieczone usługi środowiska Systemu OT, pozwalające przysyłać hasła w postaci niezabezpieczonej (np. telnet lub ftp), nie powinny być wykorzystywane.
- 2.6.8. Zabronione jest podłączanie do Sieci OT innych zasobów niż zasoby Systemu OT.
- 2.6.9. Zabrania się w Obiektach OT samodzielnych modyfikacji, ingerencji, zmiany lokalizacji lub połączeń Urządzeń OT do Sieci OT bez uzyskania zgody Inżyniera OT.
- 2.6.10. Pracownicy Podmiotów zewnętrznych nie mogą podłączać w Obiektach OT żadnych Urządzeń OT do Sieci OT bez uzyskania zgody Inżyniera OT.
- 2.6.11. Konfiguracja urządzeń aktywnych Sieci OT powinna być prowadzona zgodnie z uznaną praktyką w tym zakresie, formalnie dokumentowana oraz okresowo weryfikowana.
- 2.6.12. Dostęp do Systemu OT spoza Sieci OT (z wyłączeniem Internetu) powinien być możliwy wyłącznie dla autoryzowanych usług i Użytkowników OT z wykorzystaniem autoryzowanych protokołów i środków uwierzytelniających.
- 2.6.13. Dostęp do Internetu z Sieci OT musi być ograniczony. Ruch może być dopuszczony na potrzeby licencyjne, instalacji poprawek itd. Wymagane jest filtrowanie i ograniczanie ruchu do niezbędnego minimum.
- 2.6.14. Aplikacje webowe działające w Sieci OT muszą być zabezpieczone przed atakami sieciowymi.
- 2.6.15. W Sieci OT nie powinny być używane nieszyfrowane protokoły komunikacyjne (np. http, FTP).

2.7. Sieć bezprzewodowa Systemu OT

- 2.7.1. Sieć bezprzewodowa Systemu OT musi być przeznaczona wyłącznie dla funkcjonowania dedykowanych Systemów informatycznych OT lub Urządzeń OT, których architektura tego wymaga. Wykorzystywanie sieci bezprzewodowej dla innych celów jest zabronione. W tym celu powinny być zaimplementowane odpowiednie metody uwierzytelnienia oraz szyfrowania transmisji danych.
- 2.7.2. Sieć bezprzewodowa Systemu OT powinna być wydzieloną siecią w dedykowanym APN prywatnym z ograniczonym dostępem.
- 2.7.3. Punkty dostępowe powinny być umieszczone tak, aby w miarę możliwości uniemożliwić dostęp do sieci bezprzewodowej Systemów OT spoza obszaru PSG, w szczególności z obszaru publicznie dostępnego.

- 2.7.4. W celu utrudnienia nieautoryzowanego dostępu poprzez urządzenie mobilne należy zapewnić wymuszenie uwierzytelnienia Użytkownika OT przed uzyskaniem dostępu do sieci bezprzewodowej.
- 2.7.5. Przesyłane za pomocą sieci bezprzewodowej Systemów OT informacje powinny podlegać ochronie w celu zapewnienia poufności i integralności poprzez wykorzystanie odpowiednich mechanizmów kryptograficznych.

2.8. Urządzenia mobilne w Systemie OT

- 2.8.1. Urządzenia mobilne wykorzystywane w Systemie OT muszą być autoryzowane przez Departament Teleinformatyki i Cyberbezpieczeństwa.
- 2.8.2. Urządzenia mobilne wykorzystywane w Systemie OT podlegają ogólnym zasadom eksploatacji, zabezpieczeń i konfiguracji stosowanych w PSG.
- 2.8.3. Urządzenia mobilne wykorzystywane w Systemie OT muszą mieć aktywną ochronę antywirusową wraz z najnowszą bazą wirusów, a zainstalowany system operacyjny powinien być wspierany przez producenta oraz zaktualizowany.
- 2.8.4. Urządzenia mobilne wykorzystywane w Systemie OT powinny być zabezpieczone przed nieautoryzowanym załogowaniem się.
- 2.8.5. Do korzystania z urządzeń mobilnych w Systemie OT autoryzowani są Inżynierowie OT.
- 2.8.6. Inżynierowie OT są odpowiedzialni za konfigurację i używanie urządzeń mobilnych zgodnie z Zasadami.

2.9. Zarządzanie oprogramowaniem w Systemie OT

- 2.9.1. Systemy informatyczne OT oraz Urządzenia OT powinny być wyposażone w środki zapewniające odpowiedni poziom bezpieczeństwa teleinformatycznego (np. kontrolę dostępu, minimalizację wpływu szkodliwego oprogramowania).
- 2.9.2. Oprogramowanie Systemów informatycznych OT lub Urządzeń OT powinno być regularnie aktualizowane oraz uprzednio przetestowane.
- 2.9.3. Użytkownik OT nie może instalować w Systemie OT oprogramowania innego niż jest dopuszczone do eksploatacji na danym Systemie informatycznym OT lub Urządzeniu OT.
- 2.9.4. Instalacja oprogramowania w Systemie OT może być wykonywana tylko przez Inżyniera OT.
- 2.9.5. Użytkownik OT nie może dokonywać żadnych zmian konfiguracyjnych w Systemach informatycznych OT lub Urządzeniach OT.
- 2.9.6. Zmiany w zakresie konfiguracji komponentów oraz funkcjonalności Systemów informatycznych OT lub Urządzeń OT mogą być dokonywane jedynie przez Inżyniera OT.
- 2.9.7. Instalowanie / odinstalowywanie, uruchamianie / wyłączanie oprogramowania w Systemie OT musi uwzględniać aspekty prawidłowego, ciągłego działania Systemu OT.

- 2.9.8. Proces instalowania / odinstalowywania oraz uruchamiania / wyłączania oprogramowania w Systemie OT w zakresie cyberbezpieczeństwa Systemu OT może być inicjowany po akceptacji Biura Bezpieczeństwa Teleinformatycznego.

2.10. Ochrona Systemu OT przed szkodliwym oprogramowaniem

- 2.10.1. Zastosowanie zabezpieczenia ochrony antywirusowej oraz ochrony antymalware powinny być adekwatne dla Systemu OT i uwzględniać aspekty techniczne Systemu OT.
- 2.10.2. Ochrona antywirusowa oraz ochrona antymalware swoim obszarem powinna obejmować wszystkie komponenty Systemu OT, które technicznie i organizacyjnie umożliwiają stosowanie takich zabezpieczeń. Dla Urzędzeń OT jej implementacja może być utrudniona bez dodatkowych urządzeń i nakładów finansowych.
- 2.10.3. Oprogramowanie antywirusowe oraz oprogramowanie antymalware użyte do ochrony Systemu OT musi być odpowiednio skonfigurowane, aby chronić je przed zagrożeniami ze strony szkodliwego oprogramowania, a jednocześnie, aby nie powodowało komplikacji w prawidłowym działaniu Systemu OT.
- 2.10.4. Oprogramowanie antywirusowe oraz oprogramowanie antymalware użyte do ochrony Systemu OT powinno być przetestowane uwzględniając aspekty prawidłowego działania Systemu OT.

2.11. Elektroniczne nośniki informacji w Systemie OT

- 2.11.1. Konfiguracja Systemu OT powinna uniemożliwić podłączenie przez nieautoryzowane osoby elektronicznych nośników informacji do zasobów Systemu OT.
- 2.11.2. Możliwość podłączania elektronicznych nośników informacji w Systemie OT (np. pamięci pendrive i innych urządzeń USB) powinna zostać ograniczona do ściśle określonych znanych urządzeń.
- 2.11.3. Zabrania się podłączania elektronicznych nośników informacji w Systemie OT przez Pracowników podmiotów zewnętrznych.
- 2.11.4. Elektroniczne nośniki informacji dopuszczone do podłączenia w Systemie OT powinny być wykorzystywane wyłącznie do wykonywania obowiązków służbowych wynikających z obsługi Systemu OT.
- 2.11.5. Elektroniczne nośniki informacji wykorzystywane w Systemie OT powinny być zabezpieczone przed nieautoryzowanym użyciem lub szyfrowane (jeżeli Urządzenie OT obsługuje szyfrowanie danych).

2.12. Kopie bezpieczeństwa Systemu OT

- 2.12.1. Realizacja procesów związanych z wykonywaniem Kopii bezpieczeństwa nie może ograniczać funkcjonowania Systemu OT.
- 2.12.2. Sposób, zakres oraz częstotliwość tworzenia kopii bezpieczeństwa Systemów informatycznych OT powinny odzwierciedlać wymagania biznesowe, wymagania bezpieczeństwa, wymagania prawa powszechnie obowiązującego oraz stopień krytyczności przetwarzanych informacji.

- 2.12.3. Kopie bezpieczeństwa konfiguracji Urządzeń OT powinny być regularnie wykonywane oraz zabezpieczone na dedykowanych dyskach sieciowych w sposób zapewniający ich Poufność, Dostępność i Integralność.
- 2.12.4. Systemy informatyczne OT oraz konfiguracje Urządzeń OT powinny być objęte Systemem Kopii Zapasowej.
- 2.12.5. Za poprawność wykonania i weryfikację kopii bezpieczeństwa Systemu OT odpowiada Inżynier OT.

2.13. Zarządzanie zmianą w Systemie OT

- 2.13.1. Każda zmiana w Systemie OT musi być odpowiednio zaplanowana, uzgodniona z zainteresowanymi stronami, udokumentowana, zweryfikowana pod kątem bezpieczeństwa i musi być realizowana w sposób kontrolowany i przy zachowaniu formalnych zasad i procedur.
- 2.13.2. Każdy zasób Systemu OT powinien być objęty planem zarządzania aktualizacjami, definiującym harmonogram sprawdzania dostępności aktualizacji i ich instalacji.
- 2.13.3. Aktualizacja nie może obniżać poziomu bezpieczeństwa Systemu OT ani bezpieczeństwa żadnego innego elementu infrastruktury teleinformatycznej PSG.
- 2.13.4. Aktualizacje zasobów Systemu OT mogą być instalowane tylko wtedy, kiedy zostały przetestowane przez Inżyniera OT.
- 2.13.5. Dostęp do plików konfiguracyjnych Systemów informatycznych OT lub Urządzeń OT powinien być udzielony Użytkownikom OT jedynie w zakresie niezbędnym do wykonywania przez nich obowiązków służbowych.
- 2.13.6. Nieautoryzowana zmiana konfiguracji Systemów informatycznych OT lub Urządzeń OT jest zabroniona.
- 2.13.7. Konfigurację Systemów informatycznych OT lub Urządzeń OT należy poddawać okresowym przeglądom.
- 2.13.8. Za zarządzanie aktualizacjami oraz konfiguracją Systemów informatycznych OT lub Urządzeń OT odpowiedzialny jest Inżynier OT.

Załączniki:

Załącznik nr 1 – Kategoryzacja Obiektów OT

Załącznik nr 2 – Szablon karty stacji gazowej

Załącznik nr 3 – Metodyka doboru i warianty topologii Sieci OT dla stacji gazowych

Załącznik nr 4 – Wymagania techniczne dla Urządzeń komunikacyjnych OT

Załącznik nr 5 – Standardy konfiguracji dla Urządzeń komunikacyjnych OT