



Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS–OT

Standard Cyberbezpieczeństwa OT

Załącznik 1.1 Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji

Dla nowobudowanych instalacji i procesu modernizacji
systemów ICS-OT

Zatwierdził	Data	Podpis
Robert Oleński Dyrektor Biura Cyberbezpieczeństwa	15.06.2026	<i>Dokument podpisany elektronicznie dnia 2026.06.16. Oryginał dostępny w Dziale Cyberbezpieczeństwa OT.</i>
Zaakceptował	Data	Podpis
Artur Sidorko Kierownik Działu Cyberbezpieczeństwa OT	21.01.2025	<i>Dokument podpisany elektronicznie dnia 2026.06.16. Oryginał dostępny w Dziale Cyberbezpieczeństwa OT.</i>

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	2 / 26

Historia zmian dokumentu			
Wersja	Data	Osoba	Opis zmian
1.0	21.01.2019 r.	Dział Cyberbezpieczeństwa OT	Utworzenie dokumentu
2.0	15.03.2021 r.	Dział Cyberbezpieczeństwa OT	Aktualizacja dokumentu
3.0	06.02.2023 r.	Dział Cyberbezpieczeństwa OT	Aktualizacja dokumentu
4.0	20.01.2025 r.	Dział Cyberbezpieczeństwa OT	Aktualizacja dokumentu

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	3 / 26

Spis treści

1.	Cel dokumentu	5
2.	Definicje.....	5
3.	Poufność dokumentu	5
4.	Zakres stosowania	6
5.	Dokumenty powiązane	6
6.	Wymagania ogólne.....	6
6.1	Podstawowe zasady Cyberbezpieczeństwa	6
6.2	Architektura rozwiązania	7
6.3	Infrastruktura dla rozwiązań Cyberbezpieczeństwa	7
6.4	Gwarancje i wsparcie	7
6.5	Cykl życia produktu	8
6.6	Analiza Ryzyka Cyberbezpieczeństwa	8
6.7	Licencje.....	8
6.8	Przegląd Cyberbezpieczeństwa.....	8
7.	Wymagania szczegółowe.....	8
7.1	Wymagania Techniczne	8
7.1.1	Hardening komponentów ICS.....	9
7.1.2	Zarządzanie poprawkami systemu operacyjnego.....	10
7.1.3	Ochrona systemu antywirusowego	10
7.1.4	Ochrona systemu antymalware w szczególności:	11
7.1.5	Ochrona systemu AWL (Application Whitelisting)	12
7.1.6	Compliance (zgodność) systemu	13
7.1.7	Jump Server (serwer/stacja przesiadkowy).....	13
7.1.8	Autoryzacja i autentykacja (uwierzytelnienie) w szczególności:	13
7.1.9	Zbieranie Logów z systemów ICS.....	14
7.1.10	Infrastruktura fizyczna.....	15
7.1.11	Sieci ICS.....	15
7.1.12	Poświadczenia bezpieczeństwa.....	19
7.1.13	Wymiana danych z systemami zewnętrznymi	19
7.1.14	Zdalny dostęp do systemów ICS.....	19
7.1.15	Dokumentacja techniczna cyberbezpieczeństwa	20

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	4 / 26

7.1.16	Kopie zapasowe.....	21
7.1.17	Procedury	22
7.2	Testy Odbiorowe Cyberbezpieczeństwa.....	22
8.	Postanowienia końcowe.....	26
9.	Załączniki	26

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	5 / 26

1. Cel dokumentu

Dokument ten definiuje minimalne wymagania cyberbezpieczeństwa OT, które muszą być spełnione podczas: planowania, projektowania, procesu zakupowego, modernizacji, wdrożenia systemu ICS.

2. Definicje

Dane - wszelkie informacje przetwarzane w ORLEN S.A. w formie elektronicznej z wykorzystaniem dowolnych zasobów teleinformatycznych, w tym informacje podlegające ochronie w ORLEN S.A.,

ORLEN S.A. – ORLEN Spółka Akcyjna

System ICS lub OT - systemy automatyki, systemy monitorowania, systemy sterowania i systemy bezpieczeństwa obejmujące sprzęt, oprogramowanie i zasady związane z funkcjonowaniem procesów przemysłowych między innymi wszystkie stacje PC operatorskie/dyspozytorskie/inżynierskie/inne, serwery, sterowniki PLC/ESD/MMS/inne, kontrolery, urządzenia sieciowe, specjalistyczne oprogramowania, infrastruktura sieciowa,

Integralność – właściwość zapewniająca, że Systemy OT jak również Dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

Poufność – właściwość zapewniająca, że Systemy OT jak również Dane nie są udostępniane lub ujawniane w nieautoryzowany sposób,

Dostępność – właściwość zapewniająca możliwość dostępu do Systemów OT i danych zawsze wtedy, gdy jest to wymagane,

Obszar Cyberbezpieczeństwa OT ORLEN S.A. – centralna komórka organizacyjna reprezentowana w ORLEN S.A. przez Dział Cyberbezpieczeństwa OT ORLEN w Biurze Cyberbezpieczeństwa ORLEN S.A. będący właścicielem niniejszego standardu,

Obszar Cyberbezpieczeństwa OT Spółki – zespół analityków odpowiadających za cyberbezpieczeństwo OT w danej Spółce ORLEN S.A.. W przypadku braku komórki organizacyjnej zadania realizuje Obszar Cyberbezpieczeństwa OT ORLEN S.A.,

ICS lub OT - systemy automatyki, monitorowania, sterowania i bezpieczeństwa obejmujące sprzęt, oprogramowanie i zasad związanych z funkcjonowaniem procesów przemysłowych między innymi wszystkie stacje PC operatorskie/dyspozytorskie/inżynierskie/inne, serwery, sterowniki PLC/ESD/MMS/inne, kontrolery, urządzenia sieciowe, specjalistyczne oprogramowania, infrastruktura sieciowa,

Dla pozostałych terminów zastosowanie mają definicje użyte w Polityce Bezpieczeństwa Teleinformatycznego.

3. Poufność dokumentu

Niniejszy dokument stanowi własność **Obszar Cyberbezpieczeństwa OT ORLEN S.A.**. Zabrania się rozpowszechniania dokumentu osobom nieupoważnionym w sposób nie gwarantujący zachowania odpowiedniej Poufności oraz Integralności dokumentu. Na potrzeby współpracy z Partnerami zewnętrznymi Biuro Cyberbezpieczeństwa udostępnia odpowiednie załączniki i tylko one mogą być przekazywane poza Grupę ORLEN.

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	6 / 26

4. Zakres stosowania

Celem niniejszego dokumentu jest zdefiniowanie standardu cyberbezpieczeństwa dla systemów ICS-OT nowobudowanych instalacji i procesu modernizacji systemów ICS-OT w ORLEN S.A..

Niniejsze wymagania mają zastosowanie do wszystkich nowobudowanych i modernizowanych systemów ICS-OT w ORLEN S.A..

5. Dokumenty powiązane

Standard został opracowany w oparciu o niżej wymienione dokumenty:

1. Polityka Bezpieczeństwa Teleinformatycznego w Koncernie
2. Procedura zarządzania bezpieczeństwem informacji PKN Orlen
3. Narodowe Standardy Cyberbezpieczeństwa NSC 800-53
4. ISO 27001 Information technology — Security techniques — Information security management systems — Requirements
5. ISO 22301 Security and resilience — Business continuity management systems — Requirements
6. ISO 27005 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks
7. Cisco Data Center Infrastructure 2.5 Design Guide
8. NIST Cybersecurity Framework
9. Uptime Institute: "Data Center Site Infrastructure Tier Standard: Topology"
10. Uptime Institute: "Tier Standard: Operational Sustainability"
11. ANSI/TIA-942-A: "Telecommunications Infrastructure Standard for Data Centers"
12. ANSI/BICSI 002-2019: "Data Center Design and Implementation Best Practices"
13. BICSI 009-2019: "Data Center Operations and Maintenance Best Practices"
14. ANSI/TIA-606-C: "Administration Standard for Telecommunications Infrastructure"
15. EPI-DCOS „Data Centre Operations Standard"
16. ISO/IEC TS 22237 (EN-50600) „Information technology - Data center facilities and infrastructures"

6. Wymagania ogólne

6.1 Podstawowe zasady Cyberbezpieczeństwa

Wykonawca musi zaprojektować i wdrożyć środki w celu zapewnienia dostępności, integralności, poufności systemu ICS m.in.:

- a. zminimalizowanie czasu przestoju oraz szybkie przywrócenie normalnego działania w przypadku awarii, błędów lub ataków,
- b. umożliwienie dostępu do systemu ICS tylko w sposób uprawniony i autoryzowany,
- c. ochronę przed złośliwym oprogramowaniem - tam gdzie istnieje techniczna możliwość,

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	7 / 26

- d. aktualizację oprogramowania, systemów operacyjnych i oprogramowania aplikacyjnego zgodnie z zaleceniami Dostawców.

Podczas fazy projektowania wszystkie rozwiązania ICS w zakresie cyberbezpieczeństwa muszą być uzgodnione z Obszarem Cyberbezpieczeństwa OT Spółki.

6.2 Architektura rozwiązania

Architektura rozwiązania powinna być zgodna z niniejszymi wymaganiami (w tym *Zał. 1.1.4 Architektura OT*) m. in.

- a. zapewniać uniknięcie pojedynczego punktu awarii, w szczególności infrastruktury i aplikacji na poziomie wymaganym przez Komórki Biznesowe.
- b. Zapewniać segmentację sieci w celu podziału infrastruktury ICS na izolowane obszary

Architektura musi zostać pozytywnie zaakceptowana przez Obszar Cyberbezpieczeństwa OT ORLEN S.A. (na przykład: stacje operatorskie, serwery, urządzenia sieciowe).

6.3 Infrastruktura dla rozwiązań Cyberbezpieczeństwa

Dedykowana infrastruktura dla systemów cyberbezpieczeństwa musi zostać zaakceptowana przez Obszar Cyberbezpieczeństwa OT ORLEN S.A. , biorąc pod uwagę, że preferowane rozwiązania to między innymi:

- a. środowisko wirtualne
- b. zapewnienie redundantnych ścieżek komunikacji w celu zminimalizowania wpływu awarii
- c. zapewnienie redundantnych ścieżek komunikacji w celu zminimalizowania wpływu awarii
- d. rozwiązania monitorujące stan urządzeń końcowych
- e. wykorzystanie VLAN do podziału sieci

6.4 Gwarancje i wsparcie

Wykonawca zapewni, iż dostarczana infrastruktura teleinformatyczna będzie objęta wsparciem na czas określony zapisami w umowie (jeśli nie wskazano inaczej jest to okres 5 lat). W przypadku serwerów oraz komputerów gwarancja musi obejmować naprawę w miejscu instalacji jak również zachowanie dysku twardego przez Zamawiającego w przypadku konieczności jego wymiany.

Wykonawca zapewni w okresie gwarancyjnym wsparcie dla wszystkich wdrożonych rozwiązań cyberbezpieczeństwa zgodnie z zasadami opracowanymi przez Obszar Cyberbezpieczeństwa OT ORLEN S.A. w tym m.in.:

- a. wykonywanie przeglądów cyklicznych zgodnie z zapisami umowy (jeśli nie wskazano inaczej jest to nie rzadziej niż raz na pół roku) w ramach, których Wykonawca zrealizuje aktualizację rozwiązania, usunie powstałe i zgłoszone nieprawidłowości w funkcjonowaniu rozwiązania (w zakresie Hardware i Software);
- b. wykonywanie prac związanych z adresacją krytycznych podatności;

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	8 / 26

- c. doradztwo w zakresie dostarczonej konfiguracji;
- d. zapewnienie dostępu do aktualizacji zalecanych / zatwierdzonych przez producenta ICS.

6.5 Cykl życia produktu

Na etapie ofertowania potencjalny Wykonawca powinien dostarczyć dokument prezentujący cykl życia dostarczanych rozwiązań uwzględniający planowany okres świadczonego wsparcia i planowany okres zakończenia sprzedaży.

6.6 Analiza Ryzyka Cyberbezpieczeństwa

W przypadku budowy nowego rozwiązania OT / systemu OT Wykonawca jest zobligowany do wykonania Analizy Ryzyka Cyberbezpieczeństwa zgodnie ze standardem IEC 62443 oraz metodyką stosowaną w ORLEN S.A..

6.7 Licencje

W przypadku dostawy rozwiązania Wykonawca odpowiedzialny jest za dostawę wymaganych licencji niezbędnych do prawidłowego funkcjonowania rozwiązania z wyłączeniem licencji wskazanych przez Zamawiającego.

6.8 Przegląd Cyberbezpieczeństwa

Obszar Cyberbezpieczeństwa OT ORLEN S.A. jest uprawniony do wykonania przeglądu cyberbezpieczeństwa rozwiązań wdrażanych przez Wykonawcę, między innymi:

- a. skanowanie podatności,
- b. weryfikację ruchu sieciowego,
- c. weryfikację konfiguracji,
- d. weryfikację zainstalowanych rozwiązań,
- e. weryfikację hardeningu komponentów ICS.

Wykonawca jest zobowiązany do zapewnienia niezbędnego wsparcia w trakcie przeglądu cyberbezpieczeństwa oraz do niezwłocznego usunięcia niezgodności i wykrytych zagrożeń.

7. Wymagania szczegółowe

7.1 Wymagania Techniczne

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	9 / 26

7.1.1 Hardening komponentów ICS

Wykonawca zobligowany jest wdrożyć rozwiązania oparte o zasadę wielowarstwowego cyberbezpieczeństwa oraz wykonać wszelkie prace, które zapewnią:

- a. Każdy dostęp logiczny do portów USB, z wyłączeniem klawiatury oraz urządzeń wskazujących interfejsu graficznego (np. trackball, mysz) musi być zablokowany, w tym w szczególności w zakresie nośników pamięci, dysków przenośnych, stacji dyskiek, CD / DVD, złącz kart pamięci itp.
- b. Należy uruchomić i skonfigurować firewall-e dostępne z poziomu systemu operacyjnego lub systemu antywirusowego tak, aby dostępne były jedynie usługi i porty, które są wykorzystywane w trakcie eksploatacji systemu ICS oraz systemów cyberbezpieczeństwa.
- c. Nieużywane aplikacje muszą być odinstalowane (jedynie aplikacje niezbędne do prawidłowej eksploatacji systemu ICS).
- d. Niewykorzystane usługi powinny być wyłączone (np. w systemie operacyjnym).
- e. Niewykorzystywane karty sieciowe muszą być wyłączone.
- f. Niewykorzystywane zasoby sieciowe (np. udostępnianie plików lub folderów za pośrednictwem sieci) powinny być usunięte (jedynie niezbędne zasoby i uprawnienia do prawidłowego funkcjonowania systemu ICS).
- g. Ustawień BIOS/UEFI (w tym ustawienia hasła dostępowego, brak możliwości uruchomienia systemu z zewnętrznego nośnika).
- h. Wyłączenie\dezaktywacja protokołów komunikacyjnych przekazujących dane logowania (np. login, hasło) w postaci niezaszyfrowanej (np. Telnet, FTP, HTTP).
- i. Usunięcie nadmiarowych członków dla grup uprzywilejowanych (np. builtin\Administrators, Schema Administrators, Domain Admins).

Dodatkowe wymagania techniczne dotyczące hardening-u najczęściej wykorzystywanych systemów operacyjnych (np. Windows & Linux) w obszarze OT ORLEN S.A. oparte są o standardy międzynarodowe przyjęte przez Obszar Cyberbezpieczeństwa OT ORLEN S.A. w tym między innymi Security Technical Implementation Guides - STIGs lub Center for Internet Security - CIS Benchmarks.

Zakres prac do wykonania opisany w załączniku technicznym uzależniony jest od:

- j. zapisów zawartych w innych elementach niniejszego standardu zakładając, że każdy taki zapis nadpisuje wymagania zawarte w wymaganiach technicznych hardening-u,
- k. wpływu zmiany konfiguracji na zapewnienie ciągłości działania systemu ICS.

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	10 / 26

7.1.2 Zarządzanie poprawkami systemu operacyjnego

- a. Systemy operacyjne / aplikacje / komponenty muszą być dostarczone, wdrożone i produkcyjnie uruchomione w najnowszej stabilnej wersji systemu i najnowszej wersji poprawek rekomendowanych przez producenta systemu ICS. Systemy operacyjne / aplikacje / komponenty muszą mieć w fazie aktywnego wsparcia producenta.
- b. W przypadku dostępności u Zamawiającego dedykowanych rozwiązań do dystrybucji poprawek dla systemów OT i możliwości jego wykorzystania dla dostarczanego rozwiązania, stacje komputerowe i serwery ICS muszą być podłączane do tego rozwiązania. W innym przypadku:
 - Dostawca musi dostarczyć, zainstalować i produkcyjnie uruchomić mechanizm umożliwiający monitorowanie i dystrybuowanie poprawek systemu operacyjnego.
 - Dostawca musi zapewnić dostęp do najnowszych zatwierdzonych poprawek systemu operacyjnego (preferowane rozwiązanie) / zalecanych przez producenta ICS w okresie gwarancyjnym.
 - Dostawca musi zapewnić bezpieczny automatyczny mechanizm uzyskiwania aktualizacji / poprawek do systemu operacyjnego zalecanych przez producenta ICS.
 - Dostawca musi zapewnić centralną konsolę zarządzania, która monitoruje aktualizacje/poprawki na wszystkich stacjach komputerowych i serwerach ICS.
 - Serwer konsoli centralnej musi być zainstalowany na infrastrukturze Zamawiającego (zapewnionej przez Zamawiającego lub dostarczonej przez Wykonawcę).
 - Dostawca musi zapewnić mechanizmy zarządzania aktualizacjami/poprawkami dla systemu operacyjnego serwerów i stacji operatorskich.
 - System zarządzania aktualizacjami/poprawkami musi być zgodny ze wszystkimi zaleceniami producenta ICS.
- c. Każdy proces aktualizacji powinien być potwierdzony i wykonany lub nadzorowany przez administratorów odpowiedzialnych za dany system ICS.
- d. Dostawca musi dostarczyć Instrukcje dotyczące systemu zarządzania aktualizacjami/poprawkami w systemie ICS

7.1.3 Ochrona systemu antywirusowego

- a. Wszystkie systemy operacyjne muszą być dostarczone, wdrożone i produkcyjnie uruchomione w najnowszej stabilnej wersji oprogramowania antywirusowego i sygnatur zalecanych przez producenta systemu ICS,

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	11 / 26

- b. Jeśli to możliwe, wszystkie stacje komputerowe oraz serwery ICS, powinny mieć wdrożone to samo oprogramowanie antywirusowe,
- c. W przypadku dostępności u Zamawiającego dedykowanego rozwiązania ochrony antywirusowej dla systemów OT i możliwości jego wykorzystania dla dostarczanego rozwiązania, stacje komputerowe i serwery ICS muszą być podłączane do tego rozwiązania. W innym przypadku:
 - Wdrażane rozwiązanie musi uzyskać akceptację Obszaru Cyberbezpieczeństwa OT ORLEN S.A. .
 - Dostawca musi dostarczyć niezbędne licencje ze wsparciem co najmniej na okres trwania gwarancji.
 - Dostawca musi zapewnić dostęp do najnowszych sygnatur antywirusowych zalecanych przez producenta ICS w okresie gwarancji.
 - Dostawca, jeżeli jest to technicznie możliwe, zapewni automatyczny mechanizm pozyskiwania sygnatur antywirusowych zalecanych przez producenta ICS. W przypadku braku takiej możliwości, Wykonawca zapewni mechanizm aktualizacji sygnatur dla oprogramowania antywirusowego serwerów i stacji operatorskich.
 - Dostawca zapewni mechanizm automatycznej dystrybucji dostępnych sygnatur antywirusowych zalecanych przez producenta ICS.
 - Oprogramowanie antywirusowe powinno mieć możliwość automatycznego (np. zgodnie z harmonogramem) i ręcznego skanowania z generowaniem raportów wyników skanowania. Automatyczne skanowanie podłączonych urządzeń peryferyjnych (np. pamięci USB) jest wymagane przed ich użyciem.
 - Zainstalowane oprogramowanie powinno mieć możliwość zdalnej konfiguracji.
 - Dostarczenie, zainstalowanie i wdrożenie centralnej konsoli zarządzającej oprogramowaniem antywirusowym na wszystkich stacjach komputerowych lub serwerach ICS.
 - Serwer konsoli centralnej musi być zainstalowany na infrastrukturze Zamawiającego (zapewnionej przez Zamawiającego lub dostarczonej przez Wykonawcę).
 - Oprogramowania umożliwia centralne zarządzanie z jednego miejsca (tj. Automatyczne zmiany w konfiguracji / aktualizacji dla wszystkich innych stacji komputerowych).
- d. Wyłączanie, odinstalowanie systemu antywirusowego z poziomu stacji komputerowych jest zabronione. Czasowe odstępstwo od tej zasady jest możliwe jedynie po akceptacji Obszaru Cyberbezpieczeństwa OT ORLEN S.A..
- e. Zmiana konfiguracji systemu antywirusowego dla ICS powinna być możliwa jedynie po akceptacji Obszaru Cyberbezpieczeństwa OT ORLEN S.A..

7.1.4 Ochrona systemu antymalware w szczególności:

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	12 / 26

- a. System antymalware wykorzystywany w ORLEN S.A. należy zainstalować na wszystkich komponentach w warstwie DMZ – tam gdzie istnieje techniczna możliwość.
- b. System antymalware wykorzystywany w ORLEN S.A. należy zainstalować na komponentach systemu ICS zaimplementowanych w warstwie sterowania/monitorowania/zabezpieczenia automatyki (np. na obiekcie), tam gdzie jego instalacja nie ma negatywnego wpływu na działanie systemu ICS.
- c. W przypadku dostępności u Zamawiającego dedykowanego rozwiązania ochrony antymalware dla systemów OT i możliwości jego wykorzystania dla dostarczanego rozwiązania, stacje komputerowe i serwery ICS muszą być podłączane do tego rozwiązania.
- d. Wyłączanie, odinstalowanie systemu antymalware z poziomu stacji komputerowych jest zabronione. Czasowe odstępstwo od tej zasady jest możliwe jedynie po akceptacji Obszaru Cyberbezpieczeństwa OT ORLEN S.A..
- e. Zmiana konfiguracji systemu antymalware dla ICS powinna być możliwa jedynie po akceptacji Obszaru Cyberbezpieczeństwa OT ORLEN S.A..

7.1.5 Ochrona systemu AWL (Application Whitelisting)

- a. Jeżeli technologicznie jest to możliwe należy objąć systemem AWL wszystkie aplikacje systemów OT.
- b. Jeśli to możliwe, wszystkie stacje komputerowe oraz serwery ICS, powinny mieć wdrożone to samo oprogramowanie AWL,
- c. w przypadku dostępności u Zamawiającego/ORLEN S.A. dedykowanego rozwiązania ochrony AWL (Application Whitelisting)) dla systemów OT i możliwości jego wykorzystania dla dostarczanego rozwiązania, stacje komputerowe i serwery ICS muszą być podłączane do tego rozwiązania . W innym przypadku:
 - Wdrażane rozwiązanie musi uzyskać akceptację Obszaru Cyberbezpieczeństwa OT Spółki.
 - Dostawca musi dostarczyć niezbędne licencje ze wsparciem co najmniej na okres trwania gwarancji.
 - Dostawca musi zapewnić dostęp do najnowszych aktualizacji zalecanych przez producenta ICS w okresie gwarancji.
 - Dostawca, jeżeli jest to technicznie możliwe, zapewni automatyczny mechanizm pozyskiwania aktualizacji zalecanych przez producenta ICS. W przypadku braku takiej możliwości, Wykonawca zapewni mechanizm aktualizacji.
 - Zainstalowane oprogramowanie powinno mieć możliwość zdalnej konfiguracji.

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	13 / 26

- Dostarczenie, zainstalowanie i wdrożenie centralnej konsoli zarządzającej oprogramowaniem AWL.
 - Serwer konsoli centralnej musi być zainstalowany na infrastrukturze Zamawiającego (zapewnionej przez Zamawiającego lub dostarczonej przez Wykonawcę).
 - Oprogramowania umożliwia centralne zarządzanie z jednego miejsca (tj. Automatyczne zmiany w konfiguracji / aktualizacji dla wszystkich innych stacji komputerowych).
- d. Wyłączanie, odinstalowanie systemu AWL z poziomu stacji komputerowych jest zabronione. Czasowe odstępstwo od tej zasady jest możliwe jedynie po akceptacji Obszaru Cyberbezpieczeństwa OT ORLEN S.A..
- e. Zmiana konfiguracji systemu AWL jest możliwa jedynie po akceptacji Obszaru Cyberbezpieczeństwa OT GK ORLEN

7.1.6 Compliance (zgodność) systemu

- a. Rozwiązanie, powinno umożliwiać wizualizację bieżącego stanu zainstalowanych aktualizacji/poprawek systemu operacyjnego wszystkich stacjach komputerowych i serwerach systemu ICS (np. raportowanie).
- b. Rozwiązanie powinno umożliwiać wizualizację bieżącego stanu bazy sygnatur antywirusowych zainstalowanego na wszystkich stacjach komputerowych i serwerach systemu ICS (np. raportowanie).

7.1.7 Jump Server (serwer/stacja przesiadkowy)

- a. Jump Server musi być zainstalowany na infrastrukturze Zamawiającego,
- b. Dostęp do Jump Server może być zrealizowany po akceptacji obszaru biznesowego oraz Obszaru Cyberbezpieczeństwa OT Spółki zgodnie ze standardem ORLEN S.A. oraz podpisaną umową.

7.1.8 Autoryzacja i autentykacja (uwierzytelnienie) w szczególności:

- a. Zdalne zarządzanie stacjami komputerowymi ICS i serwerami (w tym kontami użytkowników, zasadami haseł, dostępem itp.) powinno być realizowane przez dedykowane kontrolery domeny OT umieszczone w strefie OT.
- b. W systemie ICS muszą być zaimplementowane jedynie konta niezbędne do prawidłowej eksploatacji systemu ICS (konta nadmiarowe powinny być usunięte lub zablokowane).
- c. Domyślne konta systemu operacyjnego muszą być usunięte lub zablokowane - tam gdzie istnieje taka techniczna możliwość.
- d. Administratorzy systemu ICS muszą mieć zdefiniowane wyłącznie konta imienne.

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	14 / 26

- e. W komponentach systemu ICS pracujących pod kontrolą domeny nie powinno się stosować kont lokalnych.
- f. Zdalny dostęp do komponentów ICS może być nadawany jedynie dla indywidualnych kont dostępowych z wykluczeniem kont grupowych zgodnie z przepisami obowiązującymi w ORLEN S.A..
- g. Domyślne poświadczenia logowania muszą być zmienione przed produkcyjnym uruchomieniem systemu.
- h. Wdrożona polityka zarządzania hasłami powinna być zgodna z wymaganiami opisanymi w PBTI oraz uwzględniać konfigurację uniemożliwiającą użytkownikowi powtórne wykorzystanie ostatnich 6 haseł – tam gdzie istnieje techniczna możliwość.

7.1.9 Zbieranie Logów z systemów ICS

- a. Rozwiązanie musi zapewniać zbieranie logów ze stacji komputerowych, serwerów, urządzeń sieciowych, oprogramowania antywirusowego, macierzy dyskowych, środowiska wirtualnego systemów ICS, oprogramowania backupowego.
- b. Rozwiązanie musi umożliwiać przekazywanie logów z komponentów systemów ICS poprzez rozwiązanie (np. serwer logów) umieszczone w strefie DMZ OT do centralnej instancji systemu klasy SIEM ORLEN S.A.. Dodatkowo rozwiązanie to musi zapewniać możliwość identyfikacji źródła z którego pochodzą logi.
- c. Wraz z wdrażanym rozwiązaniem należy ustalić z Obszar Cyberbezpieczeństwa OT ORLEN S.A. a następnie opracować, przekazać i wdrożyć odpowiednią konfigurację w rozwiązaniach w zakresie:
 - logów jakie powinny być zbierane z dostarczanego/modernizowanego rozwiązania (w tym urządzeń)
 - opisanie reguł korelacyjnych logów na bazie dostępnych logów z dostarczanego/modernizowanego rozwiązania (w tym urządzeń) – Wykonawca nie oczekuje wdrożenia na Własnych systemach Cyberbezpieczeństwa,
 - opisanie, na które zdarzenia (informacje zawarte w przekazywanych logach) Wykonawca z perspektywy cyberbezpieczeństwa powinien reagować z uwzględnieniem krytyczności takich zdarzeń (np. wysoka, średnia, niska) w przypadku wdrażania systemów cyberbezpieczeństwa (np. Antywirus, Antymalware, AWL, Firewall) sposób analizy zdarzenia cyberbezpieczeństwa na bazie wdrażanych rozwiązań.
- d. Rozwiązanie musi współpracować/integrować się z rozwiązaniami klasy SIEM wiodących i uznanych producentów.
- e. Wymagania techniczne dotyczące systemu zbierania logów zawarte są w *Zał. 1.1.3 Procedura Zarządzania Logami Security OT*.

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	15 / 26

7.1.10 Infrastruktura fizyczna

- a. Wykonawca musi dokonać oznaczenia okablowanie w systemie ICS z dwóch jego końców w sposób trwały zgodnie z wykorzystywanym nazewnictwem.
- b. Zalecane jest wykonanie zasilania z dwóch niezależnych źródeł.
- c. Dokumentacja elektryczna wraz z bilansem mocy dla rozwiązań cyberbezpieczeństwa.

7.1.11 Sieci ICS

- a. Zapewnienie pełnej ochrony pomiędzy strefą IT, strefą OT DMZ i strefą OT;
 - Projektowanie i wdrażanie separacji i segmentacji sieci ICS powinno być zgodne z dokumentem *Standard Cyberbezpieczeństwa OT - Zał. 1.1.4 Architektura OT* oraz międzynarodowymi standardami cyberbezpieczeństwa takimi jak NIST, ISA/IEC 62443.
- b. Architektura sieci musi być zaakceptowana przez Obszar Cyberbezpieczeństwa OT Spółki.
- c. Wykorzystywana adresacja IP w systemach ICS musi być zgodna z adresacją wykorzystywaną w ORLEN S.A. i akceptowaną przez obszar sieciowy ORLEN S.A..
- d. Dostęp do sieci OT może być realizowany zgodnie z zasadą minimalnego dostępu i uprawnień wymaganych do realizacji funkcjonalności biznesowych i musi być zaakceptowany przez Obszar Cyberbezpieczeństwa OT Spółki.
- e. Stosowana adresacja IP powinna być unikalna na poziomie ORLEN S.A. i zaakceptowana przez pracowników obszaru sieci teleinformatycznych ORLEN S.A..
- f. Bezpośredni dostęp z sieci zewnętrznych do sieci OT (w której zaimplementowany jest system ICS) jest zabroniony.
- g. Sieci teleinformatyczne systemu ICS muszą być odseparowane od innych sieci (w tym sieci korporacyjnych) za pomocą dedykowanych firewalli.
- h. Pomiędzy sieciami OT (w których znajdują się: rozwiązania OT/Systemy OT/urządzenia OT), a sieciami IT (w których znajdują się rozwiązania IT/systemy IT/ urządzenia IT/ użytkownicy IT korporacyjnymi) muszą być odrębny segment sieci (DMZ OT), odseparowany poprzez firewall NGFW od sieci korporacyjnych oraz sieci OT.
- i. Wydzielony segment sieci (DMZ OT) musi posiadać co najmniej dedykowane podsieci dla następujących podobszarów:
 - Podsieć dla systemów cyberbezpieczeństwa OT – rozwiązania zabezpieczające, monitorujące poziom cyberbezpieczeństwa OT.
 - Podsieć dla systemów wspierających pracę Systemów OT.
 - Podsieć dedykowana do zarządzania infrastrukturą teleinformatyczną

W przypadku potrzeby zastosowania większej ilości podsieci konieczna jest akceptacja Obszar Cyberbezpieczeństwa OT ORLEN S.A.

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	16 / 26

j. Zgodnie z stosowany modelem sieci OT powinny być posegmentowane i zabezpieczone w ramach przedstawionych poniżej stref:

- Strefa 1 –Urządzenia obiektowe automatyki
 - Urządzenia sklasyfikowane w Strefie 1 mają bezpośredni wpływ na proces technologiczny. Ich poprawne funkcjonowanie jest bardzo istotne ze względu na ciągłość oraz bezpieczeństwo procesu. Bezpieczeństwo urządzeń strefy 1 powinno być zapewniane przez wykorzystanie odpowiednich mechanizmów ochrony, w tym także ochrony fizycznej.
 - Do systemów Strefy 1 zalicza się między innymi:
 - Kontrolery
 - Sterowniki PLC
 - Chromatografy
 - Mierniki
 - Wagi
 - Urządzenia wykonawcze
- Strefa 2 – Systemy automatyki
 - Urządzenia sklasyfikowane w Strefie 2 są szczególnie ważne z punktu widzenia biznesu oraz ochrony ludzi i środowiska. Urządzenia zlokalizowane w tej strefie funkcjonują w ramach systemów automatyki (DCS, SIS, SCADA), które zarządzają w sposób zautomatyzowany procesami technologicznymi, a także realizują procesy optymalizacji, akwizycji danych oraz wizualizacji procesów technologicznych.
 - Do urządzeń Strefy 2 zalicza się między innymi:
 - Serwery aplikacyjne
 - Stacje inżynierskie,
 - Stacje operatorskie/dyspozytorskie,
 - Konsole wyniesione (RTU),
 - Konsole HMI,
 - Serwer backupowy systemu DCS.
- Strefa 3 – Systemy wsparcia produkcji (DMZ OT)
 - W ramach Strefy 3 znajdują się urządzenia, które wspierają procesy technologiczne. W strefie tej znajdują się elementy systemów, które nie są krytyczne z punktu widzenia automatyki przemysłowej, ponieważ nie są odpowiedzialne za kontrolowanie krytycznych procesów technologicznych. Strefa ta pełni funkcje wydzielonego segmentu sieci (np. DMZ) pomiędzy strefami urządzeń automatyki i

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	17 / 26

systemów je kontrolujących a strefą sieci użytkowników korporacyjnych, umożliwiając wymianę danych, uzyskanie zdalnego dostępu itp.

- Do Strefy 3 zalicza się między innymi:

- Serwer plików służący do ich bezpiecznej wymiany między siecią biznesową a siecią produkcji,
- Serwer sygnatur antywirusowych,
- Rozwiązanie backupowe,

- Strefa 4 – Sieć korporacyjna

- W ramach Strefy 4 znajdują się systemy teleinformatyczne, które wspierają prace biurowe. W strefie tej znajdują się elementy systemów, których działanie nie ma wpływu na pracę systemów automatyki przemysłowej.
- Zaimplementowane są tam między innymi:
 - Systemy rachunkowo-księgowe,
 - Systemy poczty elektronicznej (np. Exchange),
 - Systemy domenowe (Active Directory) dla domeny biurowej,
 - Stacje robocze użytkowników.

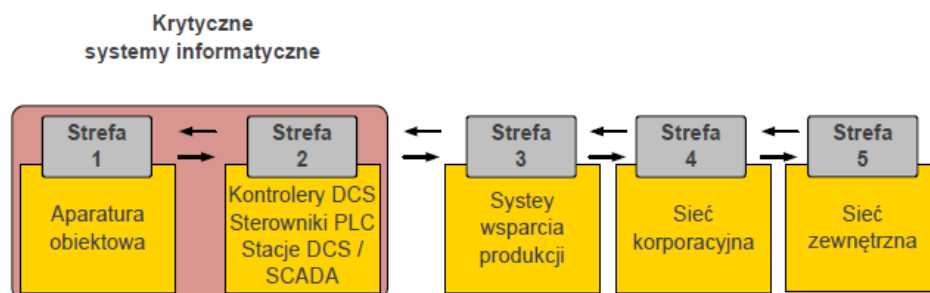
- Strefa 5 – Sieć zewnętrzna

- W Strefie 5 znajdują się systemy informatyczne, które nie są pod bezpośrednią kontrolą ORLEN.

k. Zasada przepływu danych

- Należy stosować zasadę bezpośredniego przepływu danych jedynie między sąsiadującymi strefami.
- Zgodnie z tą zasadą niedozwolone są bezpośrednie połączenia pomiędzy „odległymi strefami” np. ze strefy pierwszej jest możliwość nawiązania połączenia jedynie ze strefą drugą.
- W przypadku konieczności wymiany danych pomiędzy odległymi strefami należy przejść przez wszystkie zabezpieczenia zaimplementowana w strefach znajdujących się pomiędzy strefami źródłową i docelową. Na przykład w celu uzyskania dostępu ze Strefy 5 do Strefy 3 należy uzyskać dostęp do Strefy 4, a następnie ze Strefy 4 do Strefy 3.

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	18 / 26



- l. Sieci teleinformatyczne poszczególnych systemów ICS muszą być odseparowane od siebie, a przepływ informacji pomiędzy nimi kontrolowany.
- m. Nadmiarowy ruch generowany przez system ICS musi być usuwany u źródła tego ruchu (między innymi: ruch do sieci Internet, niewykorzystywany ruch, nadmiarowy ruch pomiędzy podsieciami, nadmiarowy ruch wewnątrz podsieci).
- n. Wszystkie urządzenia sieciowe wykorzystywane do podłączenia stacji komputerowych, serwerów, macierzy dyskowych (takich jak np.: switche, router, firewall) dostarczone do ICS muszą posiadać wszystkie porty o przepustowości min. 1 GB. Wszystkie urządzenia sieciowe dostarczane do ICS muszą być konfigurowalne: np. możliwość wyłączenia nieużywanych portów, zablokowanie nieużywanych kont oraz usług, SPAN/MIRROR port.
- o. Funkcjonalność Switch Port Analyzer (SPAN) /MIRROR PORT (umożliwiająca zrzućenie kopii ruchu sieciowego ze wszystkich innych portów do jednego portu) musi zostać skonfigurowana na urządzenia sieciowych ICS. Porty SPAN / MIRROR muszą działać bez wpływu na wydajność i poprawność działania ICS oraz umożliwiać podłączenie niezależnych rozwiązań.
- p. Zapewnienie infrastruktury, umożliwiającej przekazanie monitorowanego ruchu sieciowego w warstwach L2, L3 i L3.5 do urządzenia IDS oraz podłączanie urządzenia do sieci DMZ OT w tym:
 - Okablowania sieciowego
 - Zasilanie urządzenia
 - Miejsca montażu urządzenia
- q. W przypadku budowy nowego rozwiązania OT / systemu OT Wykonawca jest zobligowany do dostarczenia urządzeń IDS OT zgodnie ze standardem ORLEN tak aby był monitorowany cały ruch sieciowego w strefie 2 oraz 3 (warstwy L2, L2,5, L3 i L3.5).
- r. Wszystkie urządzenia sieciowe dostarczone do ICS muszą być skonfigurowane zgodnie z zasadami cyberbezpieczeństwa m.in. wyłączenie nieużywanych portów, wyłączenie nieużywanych protokołów, zablokowanie nieużywanych kont, konfiguracja urządzeń sieciowych tylko poprzez szyfrowane protokoły.

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	19 / 26

- s. Urządzenia sieciowe powinny być dostarczone, wdrożone i produkcyjnie uruchomione w najnowszej stabilnej wersji wraz z ostatnią wersją poprawek zalecanych przez producenta systemu ICS.

7.1.12 Poświadczenia bezpieczeństwa

- a. Wszystkie nazwy użytkowników muszą być przekazane do upoważnionych osób po stronie Zamawiającego wraz z przekazaniem kompletnego rozwiązania (w tym konta administratorów, konta wymagane do prac serwisowych i wszystkie inne niezbędne do działania systemu ICS).
- b. Wszystkie hasła do kont użytkowników muszą być przekazane do upoważnionych osób po stronie Zamawiającego wraz z przekazaniem rozwiązania do eksploatacji (w tym konta administratorów, konta wymagane do prac serwisowych i wszystkie inne niezbędne do działania systemu ICS) z wyłączeniem indywidualnych kont inżynierów firm trzecich.
- c. Poświadczenia bezpieczeństwa wszystkich kont administratorów z wyłączeniem indywidualnych kont inżynierów firm trzecich wykorzystywane w systemie ICS powinny być umieszczone w systemie zarządzania poświadczeniami bezpieczeństwa ORLEN S.A..

7.1.13 Wymiana danych z systemami zewnętrznymi

- a. Wymiana danych z systemami zewnętrznymi powinna odbywać się poprzez wydzieloną strefę DMZ OT.

7.1.14 Zdalny dostęp do systemów ICS

- a. Każdy dostęp zdalny do ICS może być realizowany tylko dla zdefiniowanych / indywidualnych komputerów z wykorzystaniem dedykowanego rozwiązania zainstalowanego na infrastrukturze Zamawiającego.
- b. Zdalny dostęp musi zostać zatwierdzony przez Właściciela Biznesowego oraz Obszar Cyberbezpieczeństwa OT Spółki.
- c. Zdalny dostęp musi być zgodny ze standardem i wymaganiami Obszaru Cyberbezpieczeństwa OT ORLEN S.A.. Podpisanie standardowego porozumienia ORLEN S.A. o zdalnym dostępie jest niezbędne do uruchomienia zdalnego dostępu.
- d. Zdalny dostęp do ICS jest możliwy tylko przy użyciu dedykowanego rozwiązania dopuszczonego w ORLEN S.A. przez obszar Cyberbezpieczeństwa OT ORLEN S.A.
- e. Zdalny dostęp będzie realizowany wyłącznie za pomocą rozwiązań działających w infrastrukturze ORLEN S.A. i kontrolowanych wyłącznie za pośrednictwem odpowiedzialnych administratorów ORLEN S.A..

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	20 / 26

7.1.15 Dokumentacja techniczna cyberbezpieczeństwa

- a. Wykonawca musi przekazać do zaopiniowania przez Obszar Cyberbezpieczeństwa OT Spółki niezależną dokumentację techniczną zgodną ze standardem dokumentacji cyberbezpieczeństwa (*Załącznik 1.1.1 Dokumentacja konfiguracyjna cyberbezpieczeństwa OT*).
- b. Wykonawca musi przekazać dokumentację konfiguracyjno - funkcjonalną dla dostarczanych systemów cyberbezpieczeństwa.
- c. Niezależna dokumentacja techniczna cyberbezpieczeństwa musi zawierać między innymi:
 - Architekturę połączeń pomiędzy poszczególnymi komponentami systemu i systemami zewnętrznymi obejmująca między innymi adresację, wykorzystywane numery portów i protokoły, przepływy danych.
 - Konfigurację urządzeń komputerowych, w tym między innymi:
 - ustawienia systemu operacyjnego,
 - konta użytkowników i ich uprawnienia,
 - partycjonowanie dysku z konfiguracją,
 - ustawienia kart sieciowych,
 - konfiguracja firewall-i na poziomie systemu operacyjnego lub aplikacyjnym,
 - oprogramowanie planowane / zainstalowane / uruchomione na poszczególnych zasobach wraz z rozpisaniem informacji o koniecznych do konfiguracji wyjątkach,
 - usługi (planowane / uruchomione w podziale na poszczególnych zasoby oraz aplikacje),
 - porty (planowane do otworzenia/ otwarte w podziale na poszczególne zasoby oraz aplikacje),
 - konfiguracja oprogramowania antywirusowego wraz z informacjami o koniecznych do konfiguracji wyjątkach,
 - ustawienia portów USB i napędów CD / DVD w systemie operacyjnym,
 - ustawienia BIOS/UEFI (w tym ustawienie hasła, opcja blokady uruchamiania z zewnętrznych nośników),
 - lokalne zasady bezpieczeństwa LGPO i zasady GPO,
 - procedury i polityka tworzenia kopii zapasowych,
 - lista udostępnionych zasobów sieciowych.
 - Konfigurację urządzeń sieciowych:
 - alokacja podłączonych urządzeń,

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	21 / 26

- konfiguracja portów komunikacyjnych,
 - metody dostępowe i konta,
 - konfiguracja usług systemowych.
- d.** System kopii zapasowych, w tym konfiguracja systemu backupowego, konfiguracja zasad tworzenia kopii zapasowych i ich alokacja do poszczególnych zasobów, spodziewane maksymalne obciążenie sieci, przewidywany czas utworzenia kopii zapasowej.
- e.** System antywirusowy, w tym, między innymi, jego konfiguracja w podziale na poszczególne zasoby wraz z informacjami o koniecznych do konfiguracji wyjątków.

7.1.16 Kopie zapasowe

- a.** Wykonawca musi dostarczyć kopie bezpieczeństwa (wersja źródłowa w pełni edytowalna) z finalną konfiguracją ICS, która umożliwi przywrócenie całego dostarczonego rozwiązania.
- b.** Kopie zapasowe obejmują:
- system operacyjny,
 - oprogramowanie systemowe i narzędzia programowe,
 - oprogramowanie,
 - sterowniki,
 - inne oprogramowanie niezbędne do działania ICS,
 - dane.
- c.** Jeśli to możliwe, wszystkie stacje komputerowe i serwery ICS oraz serwery, powinny mieć wdrożone to samo oprogramowanie do wykonywania kopii bezpieczeństwa.
- d.** W przypadku dostępności u Zamawiającego rozwiązań do wykonywania kopii bezpieczeństwa dla systemów OT i możliwości jego wykorzystania dla dostarczanego rozwiązania, stacje komputerowe i serwery ICS muszą być podłączane do tych rozwiązań. W innym przypadku:
- wykonawca musi dostarczyć rozwiązanie do automatycznego wykonywania backupu stacji roboczych i serwerów ICS,
 - wykonawca musi dostarczyć niezbędne licencje ze wsparciem co najmniej na okres trwania gwarancji,
 - zainstalowane oprogramowanie powinno mieć możliwość zdalnej konfiguracji,
 - wykonawca musi dostarczyć zainstalować i wdrożyć centralną konsolę zarządzającą,

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	22 / 26

- serwer konsoli centralnej musi być zainstalowany na infrastrukturze Zamawiającego (zapewnionej przez Zamawiającego lub dostarczonej przez Wykonawcę),
- oprogramowania umożliwia centralne zarządzanie z jednego miejsca (tj. Automatyczne zmiany w konfiguracji / aktualizacji dla wszystkich innych stacji komputerowych),
- system musi umożliwiać centralne: automatyczne wykonywanie backupu zgodnie z wprowadzonym planem, ręczne przywracanie i tworzenie kopii zapasowych, weryfikację poprawności wykonania kopii zapasowych i przekazywanie informacji administratorowi, dokonywanie zmian konfiguracyjnych.

7.1.17 Procedury

- Procedury tworzenia/odtworzenia kopii zapasowych.
- Procedura aktualizacji bazy szczepionek antywirusa i oprogramowania antywirusowego.
- Procedura aktualizacji systemu operacyjnego, firmware zawierająca szczegółowy opis czynności do wykonania w celu przeprowadzenia aktualizacji. Wytyczne/rekomendacje dotyczących zdarzeń cyberbezpieczeństwa, jakie powinny być monitorowane przez Zamawiającego.

7.2 Testy Odbiorowe Cyberbezpieczeństwa

- Wykonawca zobowiązany jest do zgłoszenia gotowości do odbioru wdrożonych/modernizowanych rozwiązań lub etapu zadania (w tym: ICS, cyberbezpieczeństwa) w zakresie cyberbezpieczeństwa nie później niż 2 tygodnie przed planowanym terminem odbioru wdrożonych/modernizowanych rozwiązań (np. 2 tygodnie przed zakończeniem testów SAT (Site Acceptance Test), czyli testów odbiorowych wdrożonego/zmodernizowanego rozwiązania na obiekcie).
- Warunkiem koniecznym do zgłoszenia gotowości do odbioru wdrożonych/zmodernizowanych rozwiązań lub etapu zadania jest:
 - Przekazanie kompletnej Dokumentacji Konfiguracyjnej Cyberbezpieczeństwa wszystkich przeznaczonych do odbioru komponentów wdrożonego/modernizowanego rozwiązania będącej standardem ORLEN S.A. (*Zał. 1.1.1 Dokumentacja konfiguracyjna cyberbezpieczeństwa OT*) poprzez system wymiany danych zgodny ze standardem danej Spółki,
 - Dostarczenie zrzutów konfiguracji wykonane dla wszystkich przeznaczonych do odbioru komponentów wdrożonego/modernizowanego rozwiązania (do tego celu można wykorzystać procedurę znajdującą się w *Zał. 1.1.2 Aktualna Konfiguracja Cyberbezpieczeństwa OT*) poprzez system wymiany danych zgodny ze standardem danej Spółki,

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	23 / 26

- c. Dostarczenie dodatkowych dokumentów odbiorowych (np. protokół przekazana licencji, dokumentacja funkcjonalna systemu) umożliwiających przeprowadzenie odbioru poprzez system wymiany danych zgodny ze standardem danej Spółki.
3. Zgłoszenie gotowości do odbioru należy dokonać poprzez system wymiany danych zgodny ze standardem danej Spółki oraz na adres IOT@orlen.pl
- a. W temacie wiadomości należy wpisać tekst złożonego z:
- pierwszy człon - Nazwa Spółki np. „ORLEN”,
 - drugi człon - „Testy Odbiorowy – ”,
 - trzeci człon - numer zadania inwestycyjnego np. „123456789”,
np. *ORLEN Test Odbiorowy – 123456789*,
- b. W treści wiadomości należy wpisać informację o zakresie zadania przygotowanego do odbioru np.:
- Zgłaszam do odbioru etap I zadania inwestycyjnego w ORLEN o numerze 123456789 w zakresie wymiany urządzeń sieciowych nazwa Switch 1, Switch 2 na instalacjach DRW II, DRW III.*
4. W ramach przeprowadzanych testów Wykonawca zobligowany jest do zapewnienia wsparcia Obszarowi Cyberbezpieczeństwa OT Spółki i Obszarowi Cyberbezpieczeństwa OT ORLEN S.A. przez cały okres wykonywania Testów Odbiorowych Cyberbezpieczeństwa w tym zapewnienia środowiska umożliwiającego przeprowadzenie wymaganych testów.
5. W ramach testów odbiorowych Obszar Cyberbezpieczeństwa OT Spółki / Obszar Cyberbezpieczeństwa OT ORLEN S.A. może dokonać przeglądu cyberbezpieczeństwa rozwiązań wdrożonych przez Wykonawcę między innymi:
- a. Dokonanie weryfikacji wykonanego „Hardeningu komponentów ICS (serwery, stacje, urządzenia sieciowe)” niniejszego standardu w zakresie:
- wyłączenie dostępu logicznego do portów USB, stacji dyskiek, CD / DVD,
 - wdrożenia odpowiednich zasad (konfiguracji) bezpieczeństwa cybernetycznego,
 - uruchomienia firewall-i dostępnych z poziomu systemu operacyjnego oraz ogólnej weryfikacji reguł,
 - weryfikacji czy zostały odinstalowane nieużywane aplikacje ,
 - weryfikacji czy zostały zamknięte nieużywane porty,
 - weryfikacji czy zostały wyłączone niewykorzystywane usługi i protokoły i karty sieciowe,
 - weryfikacji udostępnionych zasobów sieciowych (w tym katalogów),
 - weryfikacji zabezpieczenia BIOS (hasło, blokada uruchamiania z USB).

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	24 / 26

- b.** Dokonanie weryfikacji wdrożonego rozwiązania dla „Zarządzanie poprawkami systemu operacyjnego” niniejszego standardu w zakresie:
- zainstalowania na wszystkich wskazanych w dokumentacji cyberbezpieczeństwa stacjach operatorskich/inżynierskich, serwerach aktualnie wspieranego systemu operacyjnego, niektórych aplikacji wraz z ostatnią wersją poprawek zalecanych przez producenta systemu ICS,
 - wdrożenie rozwiązania do aktualizacji stacji komputerowych i serwerów ICS,
 - podłączenie do rozwiązania do aktualizacji wszystkich komponentów wdrażanego/modernizowanego rozwiązania.
- c.** Dokonanie weryfikacji rozwiązań w zakresie „Ochrona systemu antywirusowego z automatycznie aktualizowaną bazą szczepionek (zwalidowane sygnatury)” niniejszego standardu w zakresie:
- wdrożonej ochrony antywirusowej wraz z automatycznie aktualizowaną bazą szczepionek (zwalidowane sygnatury) w zakresie niniejszego standardu,
 - ogólnej weryfikacji polityk skanowania,
 - ogólnej weryfikacji podłączenia do rozwiązania do aktualizacji wszystkich komponentów wdrażanego/modernizowanego rozwiązania.
- d.** Dokonanie weryfikacji wdrożonej „Ochrona systemu antymalware” niniejszego standard w zakresie:
- wdrożenia rozwiązania w zakresie opisanym w niniejszego standardu,
- e.** Dokonanie weryfikacji wdrożenia „Compliance” niniejszego standard w zakresie:
- wdrożenia rozwiązania w zakresie niniejszego standardu.
- f.** Dokonanie weryfikacji wykorzystania „Jump Server” niniejszego standard w zakresie:
- wykorzystywania rozwiązania w zakresie niniejszego standardu.
- g.** Dokonanie ogólnej weryfikacji zgodności w zakresie „Autoryzacja i autentykacja” niniejszego standardu w zakresie:
- weryfikacja zablokowania lub usunięcia domyślnych kont w systemie operacyjnym,
 - weryfikacja wdrożenia imiennych kont dla administratorów systemu ICS,
 - weryfikacja stosowania lokalnych kont,
 - nadawania zdalnego dostępu do komponentów ICS jedynie dla indywidualnych kont dostępowych niniejszym standardem,
- h.** Ogólna weryfikacja wdrożenia polityk do zarządzania hasłami.

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	25 / 26

- i. Dokonanie weryfikacji wdrożenia „Systemu zbierania logów z komponentów ICS oraz przesyłania logów do centralnego rozwiązania klasy SIEM” niniejszego standardu w zakresie:
 - wdrożenia systemu zbierania logów z komponentów ICS oraz przesyłania logów do centralnego rozwiązania klasy SIEM zgodnie z wymaganiami opisanymi,
 - ogólnej weryfikacji konfiguracji polityk audytowych w zakresie rejestrowania zdarzeń zgodnie z polityką ORLEN S.A.,
 - ogólnej weryfikacji dostępności zdarzeń ze wszystkich opisanych w standardzie komponentów wdrożonego/modernizowanego rozwiązania w LogCollector,
 - j. Dokonanie weryfikacji wdrożenia wymagań Infrastruktury w zakresie:
 - wykonania oznaczeń kablowych w zakresie systemów cyberbezpieczeństwa,
 - sposób wykonania zasilania w zakresie systemów cyberbezpieczeństwa,
 - k. Wykonanie weryfikacji zastosowanej konfiguracji i architektury z obszaru sieci z perspektywy cyberbezpieczeństwa:
 - wdrożenie rozwiązania cyberbezpieczeństwa z obszaru Sieci zgodnie z wymaganiami opisanymi „Sieci” niniejszego standardu,
 - weryfikacja podłączenie do firewall IT (tak gdzie jest to wymagane),
 - ruch wychodzący (dopuszcza się jedynie zaakceptowany przez Zamawiającego ruch wychodzący z sieci rozwiązania),
 - weryfikacja portów urządzeń sieciowych,
 - weryfikacja konfiguracji SPANPORT,
 - weryfikacja konfiguracji urządzeń sieciowych zgodnie z wytycznymi dotyczącymi cyberbezpieczeństwa niniejszego standardu,
 - l. Wykonanie weryfikacji zastosowanej konfiguracji w zakresie Poświadczeń bezpieczeństwa zgodnie z wymaganiami niniejszego standardu:
 - wykonanie ogólnej weryfikacji kont systemowych w systemach operacyjnych stacji operatorskich/inżynierskich i serwerów,
 - m. Zebranie pełnej konfiguracji wszystkich dostępnych komponentów rozwiązania wykorzystując dostępne narzędzia (np. z wykorzystaniem skryptów, *Zał. 1.1.2 Aktualna Konfiguracja Cyberbezpieczeństwa OT*),
 - n. Wykonanie skanowania podatności wszystkich dostępnych komponentów rozwiązania, wykorzystując dostępne narzędzia.
6. W przypadku wykrycia przez Obszar Cyberbezpieczeństwa OT Spółki niezgodności Wykonawca zobligowany jest do ich niezwłocznego usunięcia i ponownego zgłoszenia gotowości do

	Standard Cyberbezpieczeństwa OT Wytyczne techniczne Cyberbezpieczeństwa OT do zakupów i inwestycji	Wersja:	4.0
		Data:	2025-01-21
		Strona:	26 / 26

odbioru wdrożonych/modernizowanych rozwiązań lub etapu zadania w zakresie cyberbezpieczeństwa nie później niż 2 tygodnie przed ustalonym terminem usunięcia usterek.

8. Postanowienia końcowe

Właścicielem niniejszego standardu jest Obszar Cyberbezpieczeństwa OT ORLEN S.A. Jakikolwiek zmiany lub aktualizacje w dokumencie muszą być realizowane za zgodą i przez Obszar Cyberbezpieczeństwa OT ORLEN S.A. Każda aktualizacja dokumentu musi być zaakceptowana przez osobę kierownika Obszar Cyberbezpieczeństwa OT ORLEN S.A.

9. Załączniki

1. Zał. 1.1.1 Dokumentacja konfiguracyjna cyberbezpieczeństwa OT
2. Zał. 1.1.2 Aktualna Konfiguracja Cyberbezpieczeństwa OT
3. Zał. 1.1.3 Procedura Zarządzania Logami Cyberbezpieczeństwa OT
4. Zał. 1.1.4 Architektura OT
5. Zał. 1.1.5 Dokumentacja konfiguracyjna cyberbezpieczeństwa OT – Arkusz z danymi