	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	1 z 21




## **Standard Cyberbezpieczeństwa OT**


### **Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT**

---

Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT


	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	2 z 21

Historia zmian dokumentu			
Wersja	Data	Osoba	Opis zmian
1.0	2023-12-15	Dział Cyberbezpieczeństwa OT	

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	3 z 21

## Spis treści

1.	Cel dokumentu .....	4
2.	Definicje.....	4
3.	Poufność dokumentu .....	4
4.	Zakres stosowania .....	5
5.	Dokumenty powiązane .....	5
6.	Wymagania ogólne.....	5
7.	Wymagania szczegółowe.....	7
7.1	Wymagania Techniczne.....	7
7.2	Testy Odbiorowe Cyberbezpieczeństwa .....	16
8.	Postanowienia końcowe.....	20
9.	Załączniki .....	20

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	4 z 21

## 1. Cel dokumentu

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

## 2. Definicje

**Dane** - wszelkie informacje przetwarzane w Grupie ORLEN w formie elektronicznej z wykorzystaniem dowolnych zasobów teleinformatycznych, w tym informacje podlegające ochronie w Grupie ORLEN,

**Grupa ORLEN** – ORLEN S.A. oraz spółki, w których ORLEN S.A. posiada zaangażowanie kapitałowe,

**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 Grupy ORLEN** – centralna komórka organizacyjna reprezentowana w Grupie ORLEN 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 Grupy ORLEN. W przypadku braku komórki organizacyjnej zadania realizuje Obszar Cyberbezpieczeństwa OT Grupy ORLEN,

**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 GK ORLEN**. 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.

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	5 z 21

## 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 Grupie ORLEN.


## 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

1. Wykonawca musi zaprojektować i wdrożyć środki w celu zapewnienia dostępności, integralności, poufności systemu ICS m.in:
  - a. zminimalizowanie czasu przestojów 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,

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	6 z 21

- d. aktualizację oprogramowania, systemów operacyjnych i oprogramowania aplikacyjnego zgodnie z zaleceniami Dostawców.
2. Podczas fazy projektowania wszystkie rozwiązania ICS w zakresie cyberbezpieczeństwa muszą być uzgodnione z Obszarem Cyberbezpieczeństwa OT Spółki.
3. Architektura rozwiązania powinna być zgodna z niniejszymi wymaganiami (w tym Załącznikiem nr 5 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 Grupy ORLEN (na przykład: stacje operatorskie, serwery, urządzenia sieciowe).
4. Dedykowana infrastruktura dla systemów cyberbezpieczeństwa musi zostać zaakceptowana przez Obszar Cyberbezpieczeństwa OT Grupy ORLEN , biorąc pod uwagę, że preferowane rozwiązania to między innymi:
  - a. środowisko wirtualne
  - b. zapewnienie redundantnych ścieżek komunikacji w celu zminimalizowania wpływu awarii
  - c. rozwiązania monitorujące stan urządzeń końcowych
  - d. wykorzystanie VLAN do podziału sieci
5. 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.
6. Wykonawca zapewni w okresie gwarancyjnym wsparcie dla wszystkich wdrożonych rozwiązań cyberbezpieczeństwa zgodnie z zasadami opracowanymi przez Obszar Cyberbezpieczeństwa OT Grupy ORLEN w tym min.: wykonywanie przeglądów cyklicznych zgodnie z zapisami umowy (jeśli nie wskazano inaczej jest to nie rzadziej niż raz na kwartał) w ramach, których Wykonawca zrealizuje aktualizację rozwiązania, usunie powstałe i zgłoszone nieprawidłowości w funkcjonowaniu rozwiązania (w zakresie Hardware i Software); wykonywanie prac związanych z adresacją krytycznych podatności; konserwację sprzętu (o ile sprzęt został dostarczony przez Wykonawcę); doradztwo w zakresie dostarczonej konfiguracji; zapewnienie dostępu do aktualizacji zalecanych / zatwierdzonych przez producenta ICS.


	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	7 z 21

7. Na etapie ofertowania potencjalny Wykonawca powinien dostarczyć dokument prezentujący cykl życia dostarczanych rozwiązań uwzględniający planowany okres świadczonego wsparcia i planowany okres zakończenia sprzedaży.
8. W przypadku dostawy rozwiązania Wykonawca odpowiedzialny jest za dostawę wymaganych licencji niezbędnych do prawidłowego funkcjonowania rozwiązania z wyłączeniem licencji wskazanych przez Zamawiającego.
9. Obszar Cyberbezpieczeństwa OT Spółki i Obszar Cyberbezpieczeństwa OT Grupy ORLEN są uprawnieni 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.
10. Wykonawca jest zobowiązany do zapewnienia niezbędnego wsparcia w trakcie przeglądu cyberbezpieczeństwa oraz do niezwłocznego usunięcia niezgodności i wykrytych zagrożeń.
11. Wykonawca jest zobligowany do przestrzegania zasad cyberbezpieczeństwa ujętych w niniejszym standardzie w szczególności w załączniku nr 4 do Standardu Cyberbezpieczeństwa OT - Wyciąg z Polityki Bezpieczeństwa Teleinformatycznego w Koncernie dla stron trzecich.

## 7. Wymagania szczegółowe

### 7.1 Wymagania Techniczne

1. Wykonawca zobligowany jest wdrożyć rozwiązania oparte o zasadę wielowarstwowego cyberbezpieczeństwa oraz wykonać wszelkie prace, które zapewnią:
  - a. Hardening komponentów ICS (serwery, stacje, urządzenia sieciowe) opierający się na podstawowych założeniach takich jak:
    - i. 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 dyskietek, CD / DVD, złącz kart pamięci itp.

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	8 z 21


- ii. 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.
- iii. Nieużywane aplikacje muszą być odinstalowane (jedynie aplikacje niezbędne do prawidłowej eksploatacji systemu ICS).
- iv. Niewykorzystane usługi powinny być wyłączone (np. w systemie operacyjnym).
- v. Niewykorzystywane karty sieciowe muszą być wyłączone.
- vi. Niewykorzystywane zasoby sieciowe (np. udostępnianie plików lub folderów za pośrednictwem sieci) powinny być usunięte (jedynie niezbędne zasoby i uprawnienia do prawidłowego funkcjonowania systemu ICS).
- vii. Ustawień BIOS/UEFI (w tym ustawienia hasła dostępowego, brak możliwości uruchomienia systemu z zewnętrznego nośnika).
- viii. Wyłączenie\dezaktywacja protokołów komunikacyjnych przekazujących dane logowania (np. login, hasło) w postaci niezaszyfrowanej (np. Telnet, FTP, HTTP).
- ix. Usunięcie nadmiarowych członków dla grup uprzywilejowanych (np. builtin\Administrators, Schema Administrators, Domain Admins).

Dodatkowe wymagania techniczne dotyczące hardening-u najczęściej wykorzystywanych systemów operacyjnych w obszarze OT Grupy ORLEN oparte są o standardy międzynarodowe przyjęte przez Obszar Cyberbezpieczeństwa OT Grupy ORLEN.


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

- x. zapisów zawartych w innych elementach niniejszego standardu zakładając że każdy taki zapis nadpisuje wymagania zawarte w wymaganiach technicznych hardening-u,
  - xi. wpływu zmiany konfiguracji na zapewnienie ciągłości działania systemu ICS.
- b. Zarządzanie poprawkami systemu operacyjnego w szczególności:**
- i. systemy operacyjne oraz aplikacje muszą być dostarczone, wdrożone i produkcyjnie uruchomione w najnowszej stabilnej wersji systemu i najnowszej wersji poprawek rekomendowanych przez producenta systemu ICS,
  - ii. 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 musi być podłączane do tego rozwiązania. W innym przypadku:
    - Wykonawca musi dostarczyć, zainstalować i produkcyjnie uruchomić mechanizm umożliwiający monitorowanie i dystrybuowanie poprawek systemu operacyjnego.




	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	9 z 21

- Wykonawca musi zapewnić dostęp do najnowszych zatwierdzonych poprawek systemu operacyjnego (preferowane rozwiązanie) / zalecanych przez producenta ICS w okresie gwarancyjnym.
  - Wykonawca musi zapewnić bezpieczny automatyczny mechanizm uzyskiwania aktualizacji / poprawek do systemu operacyjnego zalecanych przez producenta ICS.
  - Wykonawca 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).
  - Wykonawca 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.
- iii. Każdy proces aktualizacji powinien być potwierdzony i wykonany lub nadzorowany przez administratorów odpowiedzialnych za dany system ICS.
- iv. Wykonawca musi dostarczyć Instrukcje dotyczące systemu zarządzania aktualizacjami/poprawkami w systemie ICS
- c. Ochrona systemu antywirusowego z automatycznie aktualizowaną bazą szczepionek (zwalidowane sygnatury) w szczególności:
- i. wszystkie systemy operacyjne muszą być dostarczone, wdrożone i produkcyjnie uruchomione w najnowszej stabilnej wersji oprogramowania antywirusowego i sygnatur zalecanych przez producenta systemu ICS,
  - ii. jeśli to możliwe, wszystkie stacje komputerowe oraz serwery ICS, powinny mieć wdrożone to samo oprogramowanie antywirusowe,
  - iii. 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 (obecnie dostępne rozwiązanie to Symantec). W innym przypadku:
- Wdrażane rozwiązanie musi uzyskać akceptację Obszaru Cyberbezpieczeństwa OT Spółki.
  - Wykonawca musi dostarczyć niezbędne licencje ze wsparciem co najmniej na okres trwania gwarancji.
  - Wykonawca musi zapewnić dostęp do najnowszych sygnatur antywirusowych zalecanych przez producenta ICS w okresie gwarancji.

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	10 z 21

- Wykonawca, 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.
  - Wykonawca 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).
- iv.** Wyłączanie, odinstalowanie systemu antywirusowego z poziomu stacji komputerowych jest zabronione. Czasowe odstępstwo od tej zasady jest możliwe jedynie po akceptacji Obszaru Cyberbezpieczeństwa OT Spółki.
- v.** Zmiana konfiguracji systemu antywirusowego dla ICS powinna być możliwa jedynie po akceptacji Obszaru Cyberbezpieczeństwa OT Spółki.
- d.** Ochrona systemu antymalware w szczególności:
- i.** System antymalware wykorzystywany w Grupie ORLEN należy zainstalować na wszystkich komponentach w warstwie DMZ – tam gdzie istnieje techniczna możliwość.
  - ii.** System antymalware wykorzystywany w Grupie ORLEN 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.
  - iii.** 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.
  - iv.** Wyłączanie, odinstalowanie systemu antymalware z poziomu stacji komputerowych jest zabronione. Czasowe odstępstwo od tej zasady jest możliwe jedynie po akceptacji Obszaru Cyberbezpieczeństwa OT Spółki.

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	11 z 21

v. Zmiana konfiguracji systemu antymalware dla ICS powinna być możliwa jedynie po akceptacji Obszaru Cyberbezpieczeństwa OT Spółki.

**e. Compliance (zgodność) systemu w szczególności:**

i. Rozwiązanie, powinno umożliwiać wizualizację bieżącego stanu zainstalowanych aktualizacji/poprawek systemu operacyjnego wszystkich stacjach komputerowych i serwerach systemu ICS (np. raportowanie).

ii. Rozwiązanie powinno umożliwiać wizualizację bieżącego stanu bazy sygnatur antywirusowych zainstalowanego na wszystkich stacjach komputerowych i serwerach systemu ICS (np. raportowanie).

**f. Jump Server (serwer przesiadkowy) w szczególności:**

i. Jump Server musi być zainstalowany na infrastrukturze Zamawiającego,

ii. Dostęp do Jump Server może być zrealizowany po akceptacji obszaru biznesowego oraz Obszaru Cyberbezpieczeństwa OT Spółki zgodnie ze standardem Grupy ORLEN oraz podpisaną umową.

**g. Autoryzacja i autentykacja (uwierzytelnienie) w szczególności:**

i. 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.

ii. W systemie ICS muszą być zaimplementowane jedynie konta niezbędne do prawidłowej eksploatacji systemu ICS (konta nadmiarowe powinny być usunięte lub zablokowane).

iii. Domyślne konta systemu operacyjnego muszą być usunięte lub zablokowane - tam gdzie istnieje taka techniczna możliwość.


iv. Administratorzy systemu ICS muszą mieć zdefiniowane wyłącznie konta imienne.

v. W komponentach systemu ICS pracujących pod kontrolą domeny nie powinno się stosować kont lokalnych.


vi. Zdalny dostęp do komponentów ICS może być nadawany jedynie dla indywidualnych kont dostępowych z wykluczeniem kont grupowych zgodnie z przepisami obowiązującymi w Grupie ORLEN.

vii. Domyślne poświadczenia logowania muszą być zmienione przed produkcyjnym uruchomieniem systemu.


viii. Wdrożona polityka zarządzania hasłami powinna być zgodna z wymaganiami opisanymi w wyciągu z PBTL stanowiącym załącznik nr 4 oraz uwzględniać konfigurację uniemożliwiającą użytkownikowi powtórne wykorzystanie ostatnich 6 haseł – tam gdzie istnieje techniczna możliwość.

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	12 z 21

- h.** System zbierania logów z komponentów ICS oraz przesyłania logów do centralnego rozwiązania klasy SIEM w szczególności:
- i.** Rozwiązanie musi zapewniać zbieranie logów ze stacji komputerowych, serwerów, urządzeń sieciowych, oprogramowania antywirusowego, macierzy dyskowych, środowiska wirtualnego systemów ICS, oprogramowania backupowego.
  - ii.** 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 Grupy ORLEN. Dodatkowo rozwiązanie to musi zapewniać możliwość identyfikacji źródła z którego pochodzą logi.
  - iii.** Wraz z wdrażanym rozwiązaniem powinny być dostarczone propozycje i dobre praktyki związane z regułami korelacyjnymi, alarmowaniem i wizualizacją oraz implementowaniem źródeł.
  - iv.** Rozwiązanie musi współpracować/integrować się z rozwiązaniami klasy SIEM wiodących i uznanych producentów.
  - v.** Wymagania techniczne dotyczące systemu zbierania logów zawarte są w Załącznik nr 3 do Standardu Cyberbezpieczeństwa OT - Procedura Zarządzania Logami Security
- i.** Infrastruktura w szczególności:
- i.** Wykonawca musi dokonać oznaczenia okablowanie w systemie ICS z dwóch jego końców w sposób trwały zgodnie z wykorzystywanym nazewnictwem.
  - ii.** Zalecane jest wykonanie zasilania z dwóch niezależnych źródeł.
- j.** Sieci w szczególności:
- i.** 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 - Załącznik nr 5 - Architektura sieci OT* oraz międzynarodowymi standardami cyberbezpieczeństwa takimi jak NIST, ISA/IEC 62443.
  - ii.** Architektura sieci musi być zaakceptowana przez Obszar Cyberbezpieczeństwa OT Spółki.
  - iii.** 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.
  - iv.** Bezpośredni dostęp z sieci zewnętrznych do sieci OT (w której zaimplementowany jest system ICS) jest zabroniony.
  - v.** Sieci teleinformatyczne systemu ICS muszą być odseparowane od innych sieci (w tym sieci korporacyjnych) za pomocą dedykowanych firewalli.

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	13 z 21

- vi. Sieci teleinformatyczne poszczególnych systemów ICS muszą być odseparowane od siebie, a przepływ informacji pomiędzy nimi kontrolowany.
- vii. 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).
- viii. Wszystkie urządzenia sieciowe wykorzystywane do podłączenia stacji komputerowych, serwerów, macierzy dyskowych (takich jak np.: switch, 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.
- ix. Funkcjonalność Switch Port Analyzer (SPAN) /MIRROR PORT (umożliwiająca zrzucenie kopii ruchu sieciowego ze wszystkich innych portów do jednego portu) musi zostać skonfigurowana na urządzeniach sieciowych ICS. Porty SPAN / MIRROR muszą działać bez wpływu na wydajność i poprawność działania ICS oraz umożliwiać podłączenie niezależnych rozwiązań.
- x. 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.
- xi. Urządzenia sieciowe powinny być dostarczone, wdrożone i produkcyjnie uruchomione w najnowszej stabilnej wersji wraz z ostatnią wersją poprawek zalecanych przez producenta systemu ICS.
- k. Poświadczenia bezpieczeństwa w szczególności:
  - i. 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).
  - ii. 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.
  - iii. Poświadczenia bezpieczeństwa wszystkich kont administratorów z wyłączeniem indywidualnych kont inżynierów firm trzecich wykorzystywane w systemie ICS powinny być umieszczone w systemie zarządzania poświadczeniami bezpieczeństwa Grupy ORLEN.
- l. Wymiana danych z systemami zewnętrznymi w szczególności:
  - i. Wymiana danych z systemami zewnętrznymi powinna odbywać się poprzez wydzieloną strefę DMZ OT.

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	14 z 21


## 2. Zdalny dostęp do ICS:

- a. każdy dostęp zdalny do ICS może być realizowany tylko dla zdefiniowanych / indywidualnych komputerów z wykorzystaniem dedykowanego rozwiązania zainstalowanego na infrastrukturze Zamawiającego (np. Jump Server).
- 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 Grupy ORLEN. Podpisanie standardowego porozumienia Grupy ORLEN o zdalnym dostępie jest niezbędne do uruchomienia zdalnego dostępu.
- d. Zdalny dostęp do ICS jest możliwy tylko przy użyciu dedykowanego oprogramowania/stacji.
- e. Zdalny dostęp będzie realizowany wyłącznie za pomocą rozwiązań działających w infrastrukturze Grupy ORLEN i kontrolowanych wyłącznie za pośrednictwem odpowiedzialnych administratorów Grupy ORLEN.

## 3. Dokumentacja elektryczna wraz z bilansem mocy dla rozwiązań cyberbezpieczeństwa.

## 4. Dokumentacja techniczna cyberbezpieczeństwa:

- a. Wykonawca musi przekazać do zaopiniowania przez Obszar Cyberbezpieczeństwa OT Spółki niezależną dokumentację techniczną zgodną ze standardem dokumentacji cyberbezpieczeństwa (*Załącznik nr 1 do Standard Cyberbezpieczeństwa OT - Dokumentacja konfiguracyjna cyberbezpieczeństwa*).
- b. Wykonawca musi przekazać dokumentację konfiguracyjno - funkcjonalną dla dostarczanych systemów cyberbezpieczeństwa.
- c. Niezależna dokumentacja techniczna cyberbezpieczeństwa musi zawierać między innymi:
  - i. Architekturę połączeń pomiędzy poszczególnymi komponentami systemu i systemami zewnętrznymi obejmująca między innymi adresację, wykorzystywane numery portów i protokoły, przepływy danych.
  - ii. 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 informacjami o koniecznych do konfiguracji wyjątkach,

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	15 z 21

- usługi (planowane / uruchomione w podziale na poszczególne 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.

**iii. Konfigurację urządzeń sieciowych:**

- alokacja podłączonych urządzeń,
- konfiguracja portów komunikacyjnych,
- metody dostępowe i konta,
- konfiguracja usług systemowych.


**iv. 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.**

**v. System antywirusowy, w tym, między innymi, jego konfiguracja w podziale na poszczególne zasoby wraz z informacjami o koniecznych do konfiguracji wyjątków.**

**5. 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:
  - i.** system operacyjny,
  - ii.** oprogramowanie systemowe i narzędzia programowe,
  - iii.** oprogramowanie,
  - iv.** sterowniki,
  - v.** inne oprogramowanie niezbędne do działania ICS,



	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	16 z 21


vi. 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:
    - i. wykonawca musi dostarczyć rozwiązanie do automatycznego wykonywania backupu stacji roboczych i serwerów ICS,
    - ii. wykonawca musi dostarczyć niezbędne licencje ze wsparciem co najmniej na okres trwania gwarancji,
    - iii. zainstalowane oprogramowanie powinno mieć możliwość zdalnej konfiguracji,
    - iv. wykonawca musi dostarczyć zainstalować i wdrożyć centralną konsolę zarządzającą,
    - v. serwer konsoli centralnej musi być zainstalowany na infrastrukturze Zamawiającego (zapewnionej przez Zamawiającego lub dostarczonej przez Wykonawcę),
    - vi. oprogramowania umożliwia centralne zarządzanie z jednego miejsca (tj. Automatyczne zmiany w konfiguracji / aktualizacji dla wszystkich innych stacji komputerowych),
    - vii. 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.
6. Procedury obejmujące między innymi:
- a. Procedury tworzenia/odtworzenia kopii zapasowych.
  - b. Procedura aktualizacji bazy szczepionek antywirusa i oprogramowania antywirusowego.
  - c. 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


1. Wykonawca zobowiązany jest do zgłoszenia gotowości do odbioru wdrożonych/modernizowanych rozwiązań lub etapu zadania (w tym: ICS,



	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	17 z 21


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).

2. Warunkiem koniecznym do zgłoszenia gotowości do odbioru wdrożonych/zmodernizowanych rozwiązań lub etapu zadania jest:
  - a. przekazanie kompletnej Dokumentacji Konfiguracyjnej Cyberbezpieczeństwa wszystkich przeznaczonych do odbioru komponentów wdrożonego/modernizowanego rozwiązania będącej standardem Grupy ORLEN (Załącznik nr 1 do Standardu Cyberbezpieczeństwa OT - Dokumentacja Konfiguracyjna Cyberbezpieczeństwa OT) poprzez system wymiany danych zgodny ze standardem danej Spółki,
  - b. dostarczenie zrzutów konfiguracji wykonane dla wszystkich przeznaczonych do odbioru komponentów wdrożonego/modernizowanego rozwiązania (do tego celu można wykorzystać procedurę znajdującą się w Załączniku nr 2 do Standardu Cyberbezpieczeństwa OT – Aktualna Konfiguracja) poprzez system wymiany danych zgodny ze standardem danej Spółki,
  - c. dostarczenie dodatkowych dokumentów odbiorowych (np. protokół przekazania 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](mailto:IOT@orlen.pl)
  - a. w temacie wiadomości należy wpisać tekst złożonego z:
    - i. pierwszy człon - Nazwa Spółki np. „ORLEN”,
    - ii. drugi człon - „Testy Odbiorowy –”,
    - iii. 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 Grupy ORLEN przez cały okres wykonywania Testów Odbiorowych Cyberbezpieczeństwa w tym zapewnienia środowiska umożliwiającego przeprowadzenie wymaganych testów.


	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	18 z 21

5. W ramach testów odbiorowych Obszar Cyberbezpieczeństwa OT Spółki / Obszar Cyberbezpieczeństwa OT Grupy ORLEN może dokonać przeglądu cyberbezpieczeństwa rozwiązań wdrożonych przez Wykonawcę między innymi:

- a. dokonanie weryfikacji wykonanego „Hardeningu komponentów ICS (serwery, stacje, urządzenia sieciowe)” punkt **7.1.1.a** niniejszego standardu w zakresie:
  - i. wyłączenie dostępu logicznego do portów USB, stacji dyskiety, CD / DVD,
  - ii. wdrożenia odpowiednich zasad (konfiguracji) bezpieczeństwa cybernetycznego,
  - iii. uruchomienia firewall-i dostępnych z poziomu systemu operacyjnego oraz ogólnej weryfikacji reguł,
  - iv. weryfikacji czy zostały odinstalowane nieużywane aplikacje ,
  - v. weryfikacji czy zostały zamknięte nieużywane porty,
  - vi. weryfikacji czy zostały wyłączone niewykorzystywane usługi i protokoły i karty sieciowe,
  - vii. weryfikacji udostępnionych zasobów sieciowych (w tym katalogów),
  - viii. weryfikacji zabezpieczenia BIOS (hasło, blokada uruchamiania z USB).
- b. dokonanie weryfikacji wdrożonego rozwiązania dla „Zarządzanie poprawkami systemu operacyjnego” punkt **7.1.1.b** niniejszego standardu w zakresie:
  - i. 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,
  - ii. wdrożenie rozwiązania do aktualizacji stacji komputerowych i serwerów ICS,
  - iii. Ogólna weryfikacja podłączenia komputerów do konsoli,
  - iv. 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)” punkt **7.1.1.c** niniejszego standardu w zakresie:
  - i. wdrożonej ochrony antywirusowej wraz z automatycznie aktualizowaną bazą szczepionek (zwalidowane sygnatury) w zakresie opisanym w punkcie 1.c niniejszego standardu,
  - ii. ogólnej weryfikacji polityk skanowania,
  - iii. ogólnej weryfikacji podłączenia do rozwiązania do aktualizacji wszystkich komponentów wdrażanego/modernizowanego rozwiązania.

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	19 z 21

- d. dokonanie weryfikacji wdrożonej „Ochrona systemu antymalware” punkt **7.1.1.d** niniejszego standard w zakresie:
  - i. wdrożenia rozwiązania w zakresie opisanym w punkcie **7.1.1.d** niniejszego standardu,
- e. dokonanie weryfikacji wdrożenia „Compliance” punkt **7.1.1.e** niniejszego standard w zakresie:
  - i. wdrożenia rozwiązania w zakresie opisanym w punkcie **7.1.1.e** niniejszego standardu.
- f. dokonanie weryfikacji wykorzystania „Jump Server” punkt **7.1.1.f** niniejszego standard w zakresie:
  - i. wykorzystywania rozwiązania w zakresie opisanym w punkcie **7.1.1.f**, niniejszego standardu.
- g. dokonanie ogólnej weryfikacji zgodności w zakresie „Autoryzacja i autentykacja” punkt **7.1.1.g** niniejszego standardu w zakresie:
  - i. weryfikacja zablokowania lub usunięcia domyślnych kont w systemie operacyjnym,
  - ii. weryfikacja wdrożenia imiennych kont dla administratorów systemu ICS,
  - iii. weryfikacja stosowania lokalnych kont,
  - iv. nadawania zdalnego dostępu do komponentów ICS jedynie dla indywidualnych kont dostępowych zgodnie z punktem **7.1.1.g** niniejszym standardem,
  - v. ogólna weryfikacja wdrożenia polityk do zarządzania hasłami.
- h. dokonanie weryfikacji wdrożenia „Systemu zbierania logów z komponentów ICS oraz przesyłania logów do centralnego rozwiązania klasy SIEM” punkt **7.1.1.h** niniejszego standardu w zakresie:
  - i. wdrożenia systemu zbierania logów z komponentów ICS oraz przesyłania logów do centralnego rozwiązania klasy SIEM zgodnie z wymaganiami opisanymi w punkcie **7.1.1.h**,
  - ii. ogólnej weryfikacji konfiguracji polityk audytowych w zakresie rejestrowania zdarzeń zgodnie z polityką ORLEN S.A.,
  - iii. ogólnej weryfikacji dostępności zdarzeń ze wszystkich opisanych w standardzie komponentów wdrożonego/modernizowanego rozwiązania w LogCollector,
- i. dokonanie weryfikacji wdrożenia wymagań Infrastruktury w zakresie:
  - i. wykonania oznaczeń kablowych w zakresie systemów cyberbezpieczeństwa,
  - ii. sposób wykonania zasilania w zakresie systemów cyberbezpieczeństwa,
- j. wykonanie weryfikacji zastosowanej konfiguracji i architektury z obszaru sieci z perspektywy cyberbezpieczeństwa:

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	20 z 21

- i. wdrożenie rozwiązania cyberbezpieczeństwa z obszaru Sieci zgodnie z wymaganiami opisanymi w punkcie **7.1.1.j** „Sieci” niniejszego standardu,
- ii. weryfikacja podłączenie do firewall IT (tak gdzie jest to wymagane),
- iii. ruch wychodzący (dopuszcza się jedynie zaakceptowany przez Zamawiającego ruch wychodzący z sieci rozwiązania),
- iv. weryfikacja portów urządzeń sieciowych,
- v. weryfikacja konfiguracji SPANPORT,
- vi. weryfikacja konfiguracji urządzeń sieciowych zgodnie z wytycznymi dotyczącymi cyberbezpieczeństwa opisanymi w punkcie **7.1.1.j**,
- k. Wykonanie weryfikacji zastosowanej konfiguracji w zakresie Poświadczeń bezpieczeństwa zgodnie z wymaganiami z punktu **7.1.1.k**:
  - i. wykonanie ogólnej weryfikacji kont systemowych w systemach operacyjnych stacji operatorskich/inżynierskich i serwerów,
  - l. zebranie pełnej konfiguracji wszystkich dostępnych komponentów rozwiązania wykorzystując dostępne narzędzia (np. z wykorzystaniem skryptów dostarczonych przez Zamawiającego),
  - m. 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 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.

Jakiegokolwiek jego zmiany muszą być realizowane za zgodą i przez Obszar Cyberbezpieczeństwa.

## 9. Załączniki

1. Załącznik nr 1 do Standard Cyberbezpieczeństwa OT - Dokumentacja konfiguracyjna cyberbezpieczeństwa.
2. Załącznik nr 2 do Standard Cyberbezpieczeństwa OT – Aktualna Konfiguracja.
3. Załącznik nr 3 do Standardu Cyberbezpieczeństwa OT - Procedura Zarządzania Logami Security.
4. Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - Wyciąg z Polityki Bezpieczeństwa Teleinformatycznego w Koncernie dla stron trzecich.

	<b>Standard Cyberbezpieczeństwa OT</b>  <b>Podstawowe wymagania cyberbezpieczeństwa dla systemów ICS - OT</b>  <hr/> Dla nowobudowanych instalacji i procesu modernizacji systemów ICS - OT	Wersja:	I
		Data wydania:	2023-12-15
		Strona:	21 z 21

5. Załącznik nr 5 do Standardu Cyberbezpieczeństwa OT – Architektura OT.