



Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS-OT

Standard Cyberbezpieczeństwa OT

Załącznik 2.1 Zasady Bezpieczeństwa Teleinformatycznego OT

Zatwierdził	Data	Podpis
Robert Oleński Dyrektor Biura Cyberbezpieczeństwa	04.05.2026	<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 Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	2 / 40

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 Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	3 / 40

Spis treści

DEFINICJE.....	5
I. Definicje stosowane w niniejszym dokumencie oznaczają:	5
PREAMBUŁA	8
I. Wstęp	8
II. Cel ochrony Zasobów Teleinformatycznych IT oraz Systemów OT	8
III. Zakres stosowania	8
IV. Role i odpowiedzialność	9
OGÓLNE ZASADY CYBERBEZPIECZEŃSTWA.....	10
I. Podstawowe zasady zarządzania dostępem	10
II. Poufność i bezpieczeństwo Zasobów Teleinformatycznych IT oraz Systemów OT	10
III. Zasady zarządzania hasłami.....	10
IV. Zabezpieczenie haseł.....	11
V. Poufność i dostępność Danych.....	12
VI. Poziom Bezpieczeństwa Teleinformatycznego / Cyberbezpieczeństwa i jego weryfikacja ..	13
VII. Zasada wiedzy koniecznej	13
VIII. Wykorzystywanie Zasobów Teleinformatycznych IT oraz Systemów OT	13
IX. Bezpieczeństwo formalno-prawne.....	14
X. Polityka „czystego biurka” i Polityka „czystego ekranu”	14
XI. Ochrona przed inżynierią społeczną (socjotechniką)	15
XII. Niedozwolone czynności	15
CYBERBEZPIECZEŃSTWO OT - SYSTEMY OT	19
UŻYTKOWNICY SYSTEMÓW OT	19
I. Systemy OT - podstawowe zasady	19
II. Ochrona przed szkodliwym oprogramowaniem	19
III. Instalowanie/odinstalowywanie oraz uruchamianie/wyłączanie oprogramowania	19
IV. Sieci teleinformatyczne	20
V. Poczta elektroniczna.....	20
VI. Nośniki Elektroniczne	20
VII. Zarządzanie zmianą	20
INŻYNIEROWIE SYSTEMÓW OT	20
I. Zarządzanie dostępem do Systemów OT	20

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	4 / 40

II.	Zabezpieczenia kryptograficzne	24
III.	Zasoby Systemów OT.....	25
IV.	Model planowania, wdrożenia, utrzymania i rozwoju Systemów OT	28
V.	Sieć OT	30
VI.	Monitorowanie Systemów OT.....	33
VII.	Zarządzanie incydentami.....	33
VIII.	Zarządzanie zmianą	34
IX.	Bezpieczeństwo fizyczne i środowiskowe	35
X.	Zarządzanie ciągłością działania	36
XI.	Weryfikacja stanu cyberbezpieczeństwa	37
	INŻYNIEROWIE FIRM ZEWNĘTRZNYCH (OT) W SYSTEMACH OT	38
I.	Zasady zarządzania dostępem.....	38
II.	Ochrona przed szkodliwym oprogramowaniem	38
III.	Instalowanie/odinstalowywanie oraz uruchamianie/wyłączanie oprogramowania	39
IV.	Sieć teleinformatyczne	39
V.	Pocztą elektroniczną.....	39
VI.	Nośniki Elektroniczne	39
VII.	Zarządzanie incydentami.....	39
VIII.	Zarządzanie zmianą	40

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	5 / 40

DEFINICJE

I. Definicje stosowane w niniejszym dokumencie oznaczają:

- 1.1. **Administrator** – Użytkownik IT (administrator, programista, architekt, tester itp.) posiadający ponadstandardowe uprawnienia i obowiązki, odpowiedzialny za prawidłowe funkcjonowanie Systemu IT, utrzymanie, przeglądy, konserwację, rozwój i wdrożenia, testowanie oraz za stosowanie technicznych i organizacyjnych środków Bezpieczeństwa Teleinformatycznego.
- 1.2. **Bezpieczeństwo Teleinformatyczne / Cyberbezpieczeństwo** – stan, w którym Zasoby Teleinformatyczne mają zapewnioną ochronę przed zagrożeniami, na poziomie odpowiednim dla zdefiniowanych wymagań technicznych, biznesowych lub wymagań wynikających z przepisów prawa oraz zestaw działań i mechanizmów zapewniających tę ochronę w sposób ciągły w aspektach Poufności, Integralności, Dostępności i Rozliczalności.
- 1.3. **Dane** - wszelkie informacje przetwarzane w formie elektronicznej z wykorzystaniem dowolnych zasobów teleinformatycznych, w tym informacje podlegające ochronie w Grupie Kapitałowej ORLEN.
- 1.4. **Dostępność** – właściwość zapewniająca możliwość dostępu do Zasobów Teleinformatycznych i danych zawsze wtedy, gdy jest to wymagane.
- 1.5. **HelpDesk** – funkcjonująca w Spółce w trybie 24/7/365 telefoniczna linia wsparcia Użytkownika oraz system ServiceDesk do zgłaszania problemów i potrzeb Użytkowników.
- 1.6. **Incydent Bezpieczeństwa Teleinformatycznego / Incydent cyberbezpieczeństwa** – każde zdarzenie naruszające lub mogące prowadzić do naruszenia Bezpieczeństwa Teleinformatycznego (Cyberbezpieczeństwa), będące, w szczególności, wynikiem awarii, zaniechania (niedbałości), nieprawidłowego działania celowego, działania osób uprawnionych lub nieuprawnionych.
- 1.7. **Infrastruktura teleinformatyczna** – systemy, urządzenia, sieci teleinformatyczne, instalacje (w tym radiowe) i usługi sieciowe wykorzystywane do realizacji celów biznesowych i procesów produkcyjnych Koncernu.
- 1.8. **Integralność** – właściwość zapewniająca, że Zasoby Teleinformatyczne i Dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
- 1.9. **Inżynierowie Firm Zewnętrznych (OT)** – osoby pracujące w imieniu Stron Trzecich, świadczący usługi dla Spółki związane z Systemami OT.
- 1.10. **Inżynier OT** – Użytkownik OT będący pracownikiem Spółki, posiadający dodatkowe uprawnienia i obowiązki, odpowiedzialny za prawidłowe funkcjonowanie, utrzymanie, przeglądy, konserwację, rozwój i wdrożenia Systemów OT, testowanie oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa teleinformatycznego.
- 1.11. **Kierownik Komórki Organizacyjnej** - osoba zarządzająca zespołem pracowników i odpowiedzialna za podległy jej obszar działania Spółki, zajmująca stanowisko kierownika, dyrektora lub inne, w zależności od wewnętrznych regulacji Spółki.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	6 / 40

- 1.12. **Kierownik Utrzymania OT** - osoba będąca pracownikiem Spółki, zarządzająca zespołem Inżynierów OT i odpowiedzialna za podległy jej obszar działania Spółki, zajmująca stanowisko kierownika, dyrektora lub inne, w zależności od wewnętrznych regulacji Spółki.
- 1.13. **Koncern** – ORLEN S.A. oraz spółki, w których ORLEN S.A. posiada zaangażowanie kapitałowe.
- 1.14. **Korporacyjny Standard Informatyczny (KSI)** – opis zasad dotyczących sposobu konfiguracji sprzętu komputerowego w Koncernie obejmujący zarówno parametry techniczne, jak również podstawowe aplikacje instalowane na każdym komputerze. Podlega stałej weryfikacji oraz nadzorowi przez Dyrektora Wykonawczego ds. Informatyki Obszaru Informatyki.
- 1.15. **Nośniki Elektroniczne** – nośniki służące do zapisu i przechowywania Danych w formie elektronicznej, obejmujące zarówno urządzenia przenośne (m.in.: przenośne pamięci USB, odtwarzacze plików multimedialnych itp.) jak i nośniki będące częścią Infrastruktury Teleinformatycznej (m.in.: dyski serwerów, macierzy, urządzeń sieciowych), dyski komputerów osobistych (przenośnych i stacjonarnych), a także przenośne nośniki (np. płyty CD, DVD, Blu-ray, dyski wymienne, taśmy magnetyczne). Definicja zawiera również pamięci w Urządzeniach Mobilnych.
- 1.16. **Obszar Cyberbezpieczeństwa (IT/OT)** – wyznaczona w strukturze organizacyjnej ORLEN w Obszarze Informatyki komórka organizacyjna odpowiedzialna za Cyberbezpieczeństwo (IT oraz OT).
- 1.17. **Obszar Informatyki – Komórka Organizacyjna ORLEN, dalej Obszar IT.**
- 1.18. **OT Cybersecurity** – powołany na potrzeby całego Koncernu, centralny zespół cyberbezpieczeństwa OT w strukturze organizacyjnej Obszaru Informatyki ORLEN, w komórce organizacyjnej odpowiedzialnej za cyberbezpieczeństwo, wyznaczający standardy cyberbezpieczeństwa oraz weryfikujący cyberbezpieczeństwo procesów produkcyjnych.
- 1.19. **PBTI lub Polityka** – dokument Polityki Bezpieczeństwa Teleinformatycznego w Koncernie.
- 1.20. **Pracownicy Firm Zewnętrznych (IT)** – osoby pracujące na rzecz Stron Trzecich, świadczące usługi związane z Zasobami Teleinformatycznymi IT.
- 1.21. **Polityka „czystego biurka”** – uniemożliwienie osobom nieupoważnionym dostępu do Nośników Elektronicznych oraz dokumentów lub wydruków z systemów informatycznych, poprzez ich odpowiednie przechowywanie poza miejscem ogólnie dostępnym, w sposób uniemożliwiający zapoznanie się z nimi osobom nieupoważnionym.
- 1.22. **Polityka „czystego ekranu”** – zabezpieczanie komputerów i notebooków lub innych urządzeń służących do przetwarzania Danych poprzez stosowanie mechanizmów automatycznego blokowania dostępu po określonym czasie (np. wygaszaczy ekranu) zabezpieczonych hasłami.
- 1.23. **Poufność** – właściwość zapewniająca, że Zasób Teleinformatyczny nie jest udostępniany lub ujawniany w nieautoryzowany sposób.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	7 / 40

- 1.24. **Rozliczalność** - jedna z podstawowych funkcji Bezpieczeństwa Teleinformatycznego zapewniająca, że określone działanie jest jednoznacznie przypisane wykonującemu (użytkownikowi, procesowi, itp.). Rozliczalność zapewnia, że wszystkie działania związane z przetwarzaniem w Zasobach Teleinformatycznych umożliwiają przypisanie tych działań do wykonującego.
- 1.25. **Sieć teleinformatyczna IT (korporacyjna)** – zespół współpracujących ze sobą urządzeń informatycznych, oprogramowania oraz instalacji telekomunikacyjnych i radiowych, zapewniający wysyłanie i odbieranie danych za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego.
- 1.26. **Sieć OT** - sieć produkcyjna wykorzystywana na potrzeby komunikacji Systemów OT.
- 1.27. **Spółka** - Polski Koncern Naftowy ORLEN Spółka Akcyjna.
- 1.28. **Strony Trzecie** – podmioty współpracujące lub wykonujące prace/usługi na rzecz Spółki lub Spółek Koncernu, które posiadają dostęp do Zasobów Teleinformatycznych na podstawie podpisanych umów i zobowiązań.
- 1.29. **Systemy OT (Operational Technology) lub Systemy ICS (Industrial Control Systems) lub Zasoby teleinformatyczne OT** – wszystkie rozwiązania umożliwiające sterowanie, monitorowanie, zabezpieczanie i kontrolę infrastruktury przemysłowej wraz ze wszystkimi sieciami teleinformatycznymi służącymi do komunikacji pomiędzy komponentami danego rozwiązania stosowane w Spółce. W skład rozwiązań automatyki przemysłowej wchodzi: stacje komputerowe, serwery, sterowniki PLC, panele, kontrolery, urządzenia sieciowe, specjalistyczne urządzenia wraz z zainstalowanym na nich oprogramowaniem.
- 1.30. **Szkodliwe Oprogramowanie** – oprogramowanie, które w sposób nieautoryzowany powoduje destabilizację pracy Zasobu Teleinformatycznego, lub w inny sposób narusza Bezpieczeństwo Teleinformatyczne (w szczególności oprogramowanie o charakterze destrukcyjnym, sabotażowym, wyłudającym informacje, itp.).
- 1.31. **Urządzenia Mobilne** – urządzenia takie, jak smartphone, tablet, ewatch, inne.
- 1.32. **Użytkownik** - Użytkownik IT, Użytkownik OT lub Pracownik Firmy Zewnętrznej (IT), pracownik lub współpracownik Strony Trzeciej posiadający dostęp do Zasobów Teleinformatycznych.
- 1.33. **Użytkownik IT** – osoba uprawniona do korzystania z Zasobów Teleinformatycznych IT.
- 1.34. **Użytkownik OT** – osoba uprawniona do korzystania z Systemów OT.
- 1.35. **Właściciel Biznesowy Zasobu Teleinformatycznego (dalej: Właściciel Biznesowy IT)** – Dyrektor odpowiedzialny za wyodrębniony obszar biznesowy i z tego tytułu uprawniony do merytorycznej akceptacji dostępu do Zasobów Teleinformatycznych tego obszaru oraz akceptacji zmian, które mają kluczowe znaczenie dla tego obszaru biznesowego. Dyrektor odpowiedzialny za wyodrębniony obszar biznesowy może wyznaczyć podległego mu Kierownika Komórki Organizacyjnej, do realizacji w jego imieniu obowiązków Właściciela Biznesowego.
- 1.36. **Właściciel Biznesowy Systemu OT (dalej: Właściciel Biznesowy OT)** – Dyrektor odpowiedzialny za wyodrębniony obszar biznesowy i z tego tytułu uprawniony do merytorycznej akceptacji dostępu do Systemów OT tego obszaru oraz akceptacji

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	8 / 40

zmian, które mają kluczowe znaczenie dla tego obszaru biznesowego. Dyrektor odpowiedzialny za wyodrębniony obszar biznesowy może wyznaczyć podległego mu Kierownika Komórki Organizacyjnej, do realizacji w jego imieniu obowiązków Właściciela Biznesowego.

- 1.37. **Zasoby Teleinformatyczne IT** – systemy informatyczne, programy, aplikacje, urządzenia, infrastruktura teleinformatyczna, w tym sieci teleinformatyczne oraz usługi z wyłączeniem Systemów OT, które służą do przetwarzania Danych (w tym: wytwarzania, przechowywania lub przesyłania Danych) w Koncernie.

PREAMBUŁA

I. Wstęp

1. Niniejszy dokument został przygotowany na bazie obowiązującej Polityki Bezpieczeństwa Teleinformatycznego w Koncernie i określa zasady, do których powinni stosować się wszyscy użytkownicy oraz inżynierowie systemów OT.
2. PBTI wyznacza zasady, których spełnienie zapewni właściwy poziom Bezpieczeństwa Teleinformatycznego Zasobów Teleinformatycznych IT oraz Systemów OT w Spółce (zapewnienie Poufności, Dostępności, Integralności i Rozliczalności) jak również zapewnia zgodność działań podejmowanych w obszarze ochrony Zasobów Teleinformatycznych IT oraz Systemów OT z regulacjami prawnymi obowiązującymi na terenie Rzeczypospolitej Polskiej.
3. Zasoby Teleinformatyczne IT oraz Systemów OT Spółki mogą być wykorzystywane przez Użytkowników wyłącznie zgodnie z zasadami określonymi w PBTI oraz zgodnie z innymi obowiązującymi regulacjami wewnętrznymi i przepisami prawa powszechnie obowiązującego. Niestosowanie się do powyższych zasad może skutkować, co najmniej ograniczeniem lub odebraniem uprawnień do korzystania z poszczególnych Zasobów Teleinformatycznych IT oraz Systemów OT.
4. Spółka nie ponosi odpowiedzialności za jakiegokolwiek szkody w stosunku do Użytkowników związane z niezgodnym z niniejszą Polityką wykorzystywaniem Zasobów Teleinformatycznych IT oraz Systemów OT Spółki.

II. Cel ochrony Zasobów Teleinformatycznych IT oraz Systemów OT

1. Podstawowym celem ochrony Zasobów Teleinformatycznych IT oraz Systemów OT jest sprawne, skuteczne i spójne zarządzanie Bezpieczeństwem Teleinformatycznym/ Cyberbezpieczeństwem oparte na uznanych normach, standardach i dobrych praktykach, zapewniające realizację strategii biznesowej Spółki jak również zgodność z przepisami prawa w konsekwencji prowadzące do zapewnienia właściwego poziomu cyberbezpieczeństwa Koncernu.
2. Istotnym aspektem podejścia do ochrony Zasobów Teleinformatycznych IT oraz Systemów OT jest cyberbezpieczeństwo Systemów OT zarządzających pracą i nadzorujących instalacje i obiekty produkcji oraz dystrybucji.

III. Zakres stosowania

1. Podstawowym i nadrzędnym dokumentem w stosunku do innej dokumentacji definiującej zasady bezpieczeństwa teleinformatycznego w Spółce jest niniejsza PBTI.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	9 / 40

2. PBTI obejmuje wszystkie Zasoby Teleinformatyczne IT, Systemy OT oraz Użytkowników i zawiera zestaw reguł i ról definiujących zakresy obowiązków oraz odpowiedzialności w obszarze bezpieczeństwa Zasobów Teleinformatycznych IT oraz Systemów OT.
3. Zasady i wymagania określone w PBTI obowiązują wszystkich Użytkowników.
4. Pracownicy i współpracownicy Koncernu (osoby korzystające m.in. z komputerów będących własnością Koncernu) zobowiązani są do:
 - 4.1. Zapoznania się z treścią niniejszej Polityki.
 - 4.2. Stosowania się do obowiązujących zasad, wymagań, procedur i instrukcji w zakresie Bezpieczeństwa Teleinformatycznego/ Cyberbezpieczeństwa określonych w szczególności w niniejszej Polityce.
 - 4.3. Ukończenia dedykowanego szkolenia z zakresu PBTI na platformie e-Learning, w tym powtarzania szkolenia co dwa lata.
5. Pozostali Użytkownicy zobowiązani są do stosowania się do obowiązujących zasad, wymagań, procedur i instrukcji w zakresie Bezpieczeństwa Teleinformatycznego/ Cyberbezpieczeństwa określonych w szczególności w niniejszej Polityce.

IV. Role i odpowiedzialność

1. Wykorzystanie Zasobów Teleinformatycznych IT oraz Systemów OT niezgodnie z zasadami określonymi w PBTI, uznaje się za naruszenie przyjętych zasad bezpieczeństwa i podlega przewidzianym w takich przypadkach konsekwencjom, tj. czasowemu lub stałemu odebraniu uprawnień do Zasobów Teleinformatycznych IT i/lub Systemów OT.
2. **Strony Trzecie** - szczegółowy opis obowiązków i reguł dedykowanych dla Użytkowników znajduje się w treści PBTI. Do ich obowiązków należy również:
 - 2.1. Przestrzeganie ustalonych i przekazanych przez ORLEN zasad Bezpieczeństwa Teleinformatycznego / Cyberbezpieczeństwa, w tym zdefiniowanych przez niniejszą PBTI.
 - 2.2. Zapewnienie wykonywania obowiązków wynikających z ustaleń z ORLEN w sposób zapobiegający utracie Poufności, Integralności i Dostępności Zasobów Teleinformatycznych IT oraz Systemów OT.
 - 2.3. Zapobieganie nieuprawnionemu dostępowi do udostępnionych przez ORLEN Zasobów Teleinformatycznych IT oraz Systemów OT.
 - 2.4. Nieujawnianie aktualnych lub poprzednio używanych haseł osobistych, haseł grup roboczych oraz innych środków służących do uwierzytelniania w udostępnionych Zasobach Teleinformatycznych IT oraz Systemów OT.
 - 2.5. Korzystanie wyłącznie z zatwierdzonych przez ORLEN protokołów, usług i uprawnień.
 - 2.6. Korzystanie z udostępnionych przez ORLEN Zasobów Teleinformatycznych IT oraz Systemów OT i usług wyłącznie w celu realizacji przedmiotu umowy lub porozumienia, w zakresie zatwierdzonych uprawnień i z zachowaniem należytej staranności przy ich używaniu.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	10 / 40

- 2.7. Niezwłoczne powiadamianie o zaistniałych naruszeniach zasad lub incydentach bezpieczeństwa teleinformatycznego w związku z udzielonym dostępem do Zasobów Teleinformatycznych IT oraz Systemów OT, zgodnie z zasadami obowiązującymi w ORLEN, w tym zakresie (tu: zgłoszenie do HelpDesk ORLEN).
- 2.8. Strona Trzecia jest odpowiedzialna za skutki naruszeń bezpieczeństwa teleinformatycznego, gdy są one wynikiem nieprzestrzegania obowiązujących wymagań, zaniedbania lub niedostatecznego zabezpieczenia Zasobów Teleinformatycznych IT oraz Systemów OT przez Stronę Trzecią.

OGÓLNE ZASADY CYBERBEZPIECZEŃSTWA

I. Podstawowe zasady zarządzania dostępem

1. Użytkownicy powinni zapobiegać nieautoryzowanemu i nieuprawnionemu dostępowi, naruszeniu bezpieczeństwa, kradzieży lub uszkodzeniu Zasobów Teleinformatycznych IT oraz Systemów OT.
2. Zakres uprawnień do Zasobu Teleinformatycznego IT i Systemów OT każdego z Użytkowników powinien być ograniczony do minimalnego, niezbędnego do wykonywania obowiązków służbowych.
3. Nadanie Użytkownikowi uprawnień do poszczególnych Zasobów Teleinformatycznych IT oraz Systemów OT musi odbywać się formalnie, zgodnie z obowiązującymi regulacjami w zakresie zarządzania uprawnieniami Użytkowników.
4. Dostęp do Danych i Zasobów Teleinformatycznych IT oraz Systemów OT dla Użytkowników realizowany jest w sposób zgodny z decyzją odpowiednio Właściciela Biznesowego IT lub Właściciela Biznesowego OT i Obszaru Cyberbezpieczeństwa. Właściciel Biznesowy i Obszar Cyberbezpieczeństwa decydują, czy dostęp realizowany jest z wykorzystaniem sprzętu (komputer, smartphone, tablet, itp.) będącego własnością Koncernu lub też Użytkownika.

II. Poufność i bezpieczeństwo Zasobów Teleinformatycznych IT oraz Systemów OT

1. Wszelkie informacje o Zasobach Teleinformatycznych IT oraz Systemach OT, których ujawnienie może powodować utratę bezpieczeństwa teleinformatycznego nie powinny być ujawniane Użytkownikom ani żadnej innej nieuprawnionej osobie.
2. Nie można ujawniać informacji o charakterze, funkcjonalności, zastosowanych środkach zabezpieczeń i kontroli, sposobie ich obsługi oraz lokalizacji Zasobów Teleinformatycznych IT oraz Systemów OT osobom, które nie są uprawnione do otrzymania tego typu informacji.
3. Zabrania się udostępniania haseł do Zasobów Teleinformatycznych IT oraz Systemów OT oraz współdzielenia przypisanych do kont imiennych uprawnień. Właściciel konta imiennego odpowiedzialny jest za bezpieczeństwo konta oraz hasła i zobowiązany do okresowej zmiany haseł zgodnie z wymaganiami PBTI.

III. Zasady zarządzania hasłami

1. Użytkownicy muszą stosować hasła zgodnie z zasadami zawartymi w niniejszym rozdziale, chyba że regulacje prawne i wewnętrzne stanowią inaczej.
2. Hasła muszą być konstruowane z uwzględnieniem poniższych wymagań:

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	11 / 40

- 2.1. Długość co najmniej 10 znaków dla standardowego konta Użytkownika.
- 2.2. Długość co najmniej 14 znaków dla konta uprzywilejowanego.
- 2.3. Zastosowanie co najmniej 3 z 4 grup znaków tj. mała litera (a-z), duża litera (A-Z), cyfra (0-9), znak specjalny (np. %, #, @, &, <, ^).
3. Niedozwolone jest stosowanie haseł prostych i łatwych do odgadnięcia. Przykłady nieodpowiednich haseł:

Przykład hasła	Słabość hasła
administrator, user, nowak	hasło jako identyfikator Użytkownika
Dell, Cisco, Windows	nazwa producenta
Aaaaaaaa, mmmmm, xxxxx	powtarzanie tej samej litery
Abcdefgh,	kolejne litery
12345678, 09876543	kolejne cyfry
Komputer, zima, warszawa, jan	wyraz słownikowy
komputer1, zima4, warszawa58, jan72	prosta zmiana wyrazu słownikowego
qwerty, 1qaz2ws, asdxc,	topologiczne, wynikające z układu klawiszy na klawiaturze

4. Niedozwolone są hasła utworzone z nazw przedmiotów, czynności (hasła słownikowe), oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia, itp.).
5. W celu zwiększenia bezpieczeństwa wykorzystywanych haseł Użytkownicy powinni ignorować i anulować pojawiające się zapytania aplikacji o możliwość zapamiętania hasła.
6. W przypadku, gdy dla danego Zasobu Teleinformatycznego IT lub Systemu OT nie występuje wymaganie prawne lub wewnętrzne związane ze zdefiniowaną częstotliwością zmiany hasła, Użytkownik powinien dokonywać okresowej zmiany hasła nie rzadziej niż raz na 90 dni. Dodatkowo powinny funkcjonować zasady co do restrykcji wykorzystywania haseł używanych historycznie.
7. W przypadku wykorzystywanych przez Użytkownika kont uprzywilejowanych, hasła muszą być zmieniane nie rzadziej niż raz na 60 dni, chyba że przepisy powszechnie obowiązujące i regulacje wewnętrzne stanowią inaczej.
8. Użytkownicy mogą dokonać zmiany hasła w dowolnym momencie.
9. Użytkownik powinien niezwłocznie zmienić hasło na polecenie Administratora lub Obszaru Cyberbezpieczeństwa.

IV. Zabezpieczenie haseł

1. Haseł nie należy zapisywać i pozostawiać w miejscu, w którym mogłyby zostać ujawnione.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	12 / 40

2. Hasła nie należy przechowywać w plikach, systemach, aplikacjach, bazach danych, skryptach i plikach konfiguracyjnych bez zapewnienia im poufności środkami technicznymi lub co najmniej organizacyjnymi.
3. Hasła nie powinny być wpisywane w obecności innych osób, jeśli mogą one zauważyć treść wpisywanego hasła.
4. Bez względu na okoliczności haseł do indywidualnych kont nie wolno ujawniać. W szczególności nie należy go ujawniać przez telefon lub pocztę elektroniczną osobom, które mogą podawać się np. za pracowników pomocy technicznej.
5. Hasła do kont funkcyjnych można udostępnić wyłącznie osobom, które, zgodnie z przypisanym zakresem obowiązków, potrzebują dostępu do danego Zasobu Teleinformatycznego IT lub Zasobu Teleinformatycznego OT.
6. Hasła do kont uprzywilejowanych należy objąć szczególną ochroną.
7. Hasła należy przechowywać w sposób bezpieczny, zapewniający im poufność, dostępność oraz rozliczalność ich wykorzystania.
8. Hasła należy utrzymywać w tajemnicy również po upływie ich ważności.
9. W przypadku podejrzenia ujawnienia hasła, należy niezwłocznie skontaktować się z HelpDesk i przekazać stosowną informację.

V. Poufność i dostępność Danych

1. Nośniki Elektroniczne, muszą być zabezpieczane zgodnie z przyjętymi w Spółce zasadami.
2. Dostęp do Nośników Elektronicznych powinni posiadać tylko uprawnieni Użytkownicy lub osoby posiadające potwierdzenie z Obszaru Bezpieczeństwa IT/OT.
3. W przypadku konieczności zabrania Zasobu Teleinformatycznego IT lub Zasobu Teleinformatycznego OT do naprawy serwisowej Nośniki Elektroniczne (w tym dysk twardy) muszą zostać wymontowane przez serwisanta i pozostawione u Użytkownika IT/Użytkownika OT urządzenia. W przypadku, kiedy jest to technicznie trudne do realizacji, odstępstwa akceptowane są przez Obszar Cyberbezpieczeństwa IT/OT.
4. W przypadku uszkodzenia dysku twardego i braku możliwości odzyskania Danych na nim zawartych, dysk należy przekazać do Obszaru Informatyki w celu jego fizycznego zniszczenia w sposób zgodny z obowiązującymi procedurami.
5. W przypadku komputerów przenośnych oraz komputerów stacjonarnych w uzasadnionych przypadkach powinny być stosowane filtry prywatyzujące.
6. Wszelkie Dane przetwarzane w związku z obowiązkami służbowymi powinny być przechowywane na dedykowanych do tego celu zasobach (np. współdzielone lub indywidualne zasoby sieciowe).
7. Odpowiedzialność za właściwą Dostępność oraz Poufność Danych spoczywa na Użytkowniku przetwarzającym te Dane, w zakresie dotyczącym danego Użytkownika.
8. Zabronione jest wykorzystywanie prywatnych skrzynek pocztowych znajdujących się poza domeną pocztową ORLEN do przetwarzania Danych związanych z wykonywanymi obowiązkami służbowymi.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	13 / 40

- Do przetwarzania Danych związanych z wykonywanymi obowiązkami służbowymi wykorzystywane może być jedynie konto służbowej korporacyjnej poczty elektronicznej Koncernu.

VI. Poziom Bezpieczeństwa Teleinformatycznego / Cyberbezpieczeństwa i jego weryfikacja

- Niedozwolone jest wykorzystywanie logicznych lub sprzętowych luk w Zasobach Teleinformatycznych IT oraz Zasobach Teleinformatycznych OT.
- Zgodność konfiguracji i eksploatacji Zasobów Teleinformatycznych IT oraz Systemów OT z zasadami określonymi w PBTI może być weryfikowana przez osoby wyznaczone przez Obszar Bezpieczeństwa IT/OT.
- Użytkownicy eksploatujący Zasoby Teleinformatyczne IT lub Zasoby Teleinformatyczne OT są odpowiedzialni za zabezpieczenie wykorzystywanych komponentów przed nieuprawnionym dostępem, uszkodzeniem i utratą.
- Użytkownicy są zobowiązani do współpracy i terminowości przy prowadzonych pracach związanych bezpośrednio z Bezpieczeństwem Teleinformatycznym IT lub Zasobami Teleinformatycznymi OT dotyczących np. wgrywania uaktualnień (systemu operacyjnego, aplikacji, systemu antywirusowego).
- Wszelkie incydenty Bezpieczeństwa Teleinformatycznego / Cyberbezpieczeństwa należy niezwłocznie zgłaszać do HelpDesk.

VII. Zasada wiedzy koniecznej

- Zasada wiedzy koniecznej obowiązuje każdego Użytkownika i służy zapewnieniu, że każdy Użytkownik posiada dostęp jedynie do Zasobów Teleinformatycznych IT, Systemów OT i Danych niezbędnych mu do wykonywania obowiązków służbowych (bez uprawnień nadmiarowych).

VIII. Wykorzystywanie Zasobów Teleinformatycznych IT oraz Systemów OT

- Wszelkie działania realizowane przez Użytkowników przy wykorzystaniu Zasobów Teleinformatycznych IT oraz Systemów OT będących własnością Spółki oraz udostępnianych usług infrastruktury teleinformatycznej mają charakter służbowy, ściśle związany z realizowanymi przez Użytkowników zadaniami i w związku z tym zakłada się prawnie uzasadnioną możliwość monitorowania wszelkich podejmowanych przez Użytkowników działań z wykorzystaniem Zasobów Teleinformatycznych IT oraz Systemów OT.
- Zabronione jest pozyskiwanie, przechowywanie i rozpowszechnianie za pomocą Zasobów Teleinformatycznych IT oraz Systemów OT Spółki materiałów niezgodnych z prawem, z regulacjami wewnętrznymi, sprzecznych z interesami Spółki oraz materiałów mogących uszkodzić infrastrukturę teleinformatyczną Spółki, w szczególności oprogramowania powszechnie uznawanego za szkodliwe.
- Zabronione jest celowe usuwanie Danych, bez wyraźnej zgody Właściciela Biznesowego, przechowywanych w Zasobach Teleinformatycznych IT oraz Systemów OT Spółki. Działania takie w toku postępowań weryfikacyjnych mogą zostać uznane za działania na szkodę Spółki.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	14 / 40

4. Wszelkie materiały (np. dokumenty) wytworzone przy użyciu Zasobów Teleinformatycznych IT oraz Systemów OT Spółki stanowią własność Spółki, chyba że odrębne umowy stanowią inaczej.
5. Wykorzystywanie Zasobów Teleinformatycznych IT oraz Zasobów Teleinformatycznych, w tym poszczególnych usług informatycznych może być rejestrowane i monitorowane przez systemy i urządzenia Spółki.
6. Jedynie autoryzowane oraz uprawnione osoby mogą monitorować dzienniki zdarzeń oraz Dane z Zasobów Teleinformatycznych IT oraz Systemów OT.
7. W przypadku naruszenia zakazu przetwarzania Danych, pozostających bez związku z wykonywaniem obowiązków służbowych z wykorzystaniem Zasobów Teleinformatycznych IT oraz Systemów OT Spółki, Spółka nie jest odpowiedzialna za utratę tych Danych ani za żadne negatywne implikacje dla Użytkownika mogące wynikać z utraty poufności, integralności lub dostępności tych Danych.
8. Dane przetwarzane przez Użytkowników w formie elektronicznej z wykorzystaniem Zasobów Teleinformatycznych IT oraz Systemów OT powinny być zabezpieczone zgodnie z obowiązującymi wewnętrznymi aktami organizacyjnymi, stosownie dla przypisanej kategorii Danych, w tym Danych prawnie chronionych.

IX. Bezpieczeństwo formalno-prawne

1. Użytkownicy powinni właściwie chronić powierzone lub udostępnione im Zasoby Teleinformatyczne IT oraz Systemów OT i Dane.
2. Użytkownicy zobowiązani są do odbycia stosownego szkolenia e-Learning.
3. Na Zasobach Teleinformatycznych IT oraz Systemów OT mogą być instalowane i uruchamiane jedynie wersje programów, do których prawa autorskie lub licencje na użytkowanie są własnością ORLEN lub autoryzowane przez ORLEN oprogramowanie, które opłat za licencje nie wymaga (np. oprogramowanie typu „open source”).
4. Na Zasobach Teleinformatycznych IT oraz Systemów OT nie mogą być przechowywane pliki, do których prawa autorskie lub licencje na użytkowanie nie są własnością ORLEN (np. pliki audio, pliki wideo, zdjęcia).

X. Polityka „czystego biurka” i Polityka „czystego ekranu”

1. Polityka „czystego biurka” ma na celu zredukowanie ryzyka nieautoryzowanego i nieuprawnionego dostępu do Danych i nakłada na Użytkownika obowiązek zabezpieczenia wszelkich Danych i informacji, w tym dokumentacji papierowej i elektronicznych nośników informacji, w zależności od ich istotności w zamykanych na klucz biurkach, szafach lub sejfach podczas opuszczania stanowiska pracy.
2. Polityka „czystego ekranu” ma na celu zredukowanie ryzyka nieautoryzowanego i nieuprawnionego dostępu lub uszkodzenia Zasobów Teleinformatycznych i nakłada na Użytkownika obowiązek zabezpieczenia przed osobami postronnymi Danych aktualnie wyświetlanych na ekranie komputera oraz obowiązek

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	15 / 40

zablokowania sesji Użytkownika na komputerze, każdorazowo przy odejściu od stanowiska pracy i komputera. Zasady te obowiązują również w przypadku Urządzeń Mobilnych.

XI. Ochrona przed inżynierią społeczną (socjotechniką)

1. Użytkownicy powinni być świadomi zagrożeń związanych z wykorzystywaniem przez osoby trzecie technik manipulacji Użytkownikiem, do których należą działania zmierzające do uzyskania pożądanego przez intruza zachowania Użytkownika np. odwracanie uwagi Użytkownika od bieżącej pracy, nietypowe prośby, nietypowe zachowania.
2. Techniki wykorzystywane przez intruza przy inżynierii społecznej polegają m.in. na:
 - 2.1. Powoływaniu się na pilną sprawę o wysokim znaczeniu dla ORLEN lub innego podmiotu.
 - 2.2. Oferowaniu pomocy technicznej np. w przypadku zagrożenia wirusem komputerowym, awarią lub weryfikacją uprawnień.
 - 2.3. Próbach wymuszenia działań na Użytkowniku i powoływaniu się przy tym na osoby z wyższego szczebla, np. na przełożonego.
 - 2.4. Podszywaniu się pod inną osobę.
 - 2.5. Wzbudzeniu zaufania oraz prawieniu komplementów.
 - 2.6. Uzyskiwaniu informacji, które mogą być informacjami podlegającymi ochronie na mocy przepisów prawa np. hasła, informacje dotyczące kontrahentów lub współpracowników, informacje dotyczące stosowanych zabezpieczeń, itp.
 - 2.7. Powoływaniu się na znajomość pracowników ORLEN.
3. Zazwyczaj techniki są wykorzystywane przez osobę trzecią za pomocą dostępnych środków komunikacji, takich jak telefon, poczta elektroniczna, Internet, rzadziej osobiście.
4. W celu ochrony przed metodami socjotechniki Użytkownicy powinni zachować szczególną uwagę i w przypadku prośby o podanie informacji podlegających ochronie lub innych, których ujawnienie nieuprawnionej osobie mogłoby wyrządzić szkodę osobie przekazującej lub innej osobie czy Spółce, należy dodatkowo weryfikować zasadność prośby oraz tożsamość wnioskodawcy poprzez np. zwrotną wiadomość poczty elektronicznej, telefon.
5. W przypadku, gdy ww. weryfikacja nie potwierdzi zasadności przekazywanych Danych oraz tożsamości wnioskodawcy, należy niezwłocznie powiadomić przełożonego.

XII. Niedozwolone czynności

Poniżej określono przykładowe czynności, które, co do zasady, nie są dozwolone dla osób posiadających dostęp do Zasobów Teleinformatycznych IT lub Systemów OT. Poniższe ograniczenia mogą być wyłączone lub chwilowo zaakceptowane w przypadku zaistnienia uzasadnionej konieczności lub w przypadku wykonywania istotnych dla Spółki czynności służbowych i zatwierdzone przez Obszar Bezpieczeństwa IT/OT.

Z uwagi na ciągły rozwój technologii i rozwiązań informatycznych oraz związane z tym powstawanie nowych podatności na zagrożenia bezpieczeństwa teleinformatycznego przyjmuje się, jako nadrzędną w zakresie niedozwolonych czynności zasadę, że wszystko to, co nie jest wyraźnie dozwolone w zapisach PBTI, uważa się za zabronione.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	16 / 40

1. Systemy i sieci teleinformatyczne:

- 1.1. Ujawnienie hasła oraz pozostałe czynności umożliwiające korzystanie z Zasobów Teleinformatycznych IT lub Systemów OT przez inne, nieuprawnione osoby, np. przez członków rodziny, innych członków gospodarstwa domowego, itp.
- 1.2. Naruszenie dóbr chronionych prawem własności intelektualnej, w tym m.in. digitalizacja i dystrybucja zdjęć z czasopism, książek, utworów muzycznych i wideo, instalacja oprogramowania, wykonywanie lub dystrybucja pirackich kopii oprogramowania.
- 1.3. Nieuprawnione wprowadzanie i instalacja oprogramowania, w tym shareware, freeware lub open source.
- 1.4. Czynności związane z odgadywaniem haseł innych Użytkowników, podszywania się pod innych Użytkowników, wykorzystywanie wykrytych podatności oraz wszelkie próby przełamania lub testowania zastosowanych zabezpieczeń.
- 1.5. Omijanie wymogu uwierzytelniania Użytkownika lub zabezpieczeń jakiegokolwiek Zasobu Teleinformatycznego IT oraz Zasobu Teleinformatycznego OT (np. próby obchodzenia, dezaktywacji zabezpieczeń, itp.).
- 1.6. Powodowanie naruszenia bezpieczeństwa lub zakłócenia komunikacji w sieci teleinformatycznej Systemów OT, w tym czynności, które powszechnie uznaje się za czynności związane z nieuprawnionym przechwytywaniem pakietów i danych w sieci, próbami spowodowania odmowy usługi oraz innych uznanych w powszechnie przyjętej etyce informatycznej oraz automatyki za czynności mogące mieć szkodliwy wpływ na funkcjonowanie oraz zawartość Systemów OT.
- 1.7. Skanowanie Zasobów Teleinformatycznych IT oraz Systemów OT (komputerów, sieci komputerowych, w tym portów oraz usług teleinformatycznych) bez uzyskania niezbędnej autoryzacji na wykonywanie takich czynności od Obszaru Cyberbezpieczeństwa IT/OT.
- 1.8. Korzystanie z nieautoryzowanych komunikatorów sieciowych, w tym internetowych (tzw. chat).
- 1.9. Wykorzystywanie Zasobów Teleinformatycznych IT lub Systemów OT do innych celów niż realizacja zadań służbowych.
- 1.10. Nadużywanie posiadanych uprawnień do Zasobów Teleinformatycznych IT lub Systemów OT.
- 1.11. Celowe usuwanie Danych związanych z wykonywanymi obowiązkami służbowymi, które mogą mieć znaczenie dla ORLEN.
- 1.12. Niestosowanie należytej ochrony wobec Danych wykorzystywanych w związku z wykonywanymi obowiązkami służbowymi, w tym niewykonywanie ich kopii zapasowych oraz przechowywanie w innym miejscu niż na przeznaczonych do tego celu zasobach.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	17 / 40

- 1.13. Wykorzystywanie nieautoryzowanych przez Obszar Bezpieczeństwa IT/OT mechanizmów służących do ustanowienia zdalnego dostępu do Zasobów teleinformatycznych ORLEN.
- 1.14. Udostępnianie usługi zdalnego dostępu do Zasobów Teleinformatycznych IT lub Systemów OT osobom nieuprawnionym.
- 1.15. Udostępnianie usługi zdalnego dostępu do Zasobów Teleinformatycznych IT lub Systemów OT w sposób niezgodny z rozwiązaniami zatwierdzonymi do użytku przez Obszar Bezpieczeństwa IT/OT.
- 1.16. Przeszukiwanie udostępnionych zasobów sieciowych bez związku z wykonywaniem czynności służbowych na stanowisku pracy.

2. Komputery i urządzenia przenośne oraz Nośniki Elektroniczne

- 2.1. Pozostawianie bez nadzoru niezabezpieczonych Zasobów Teleinformatycznych IT lub Systemów OT (stacji inżynierskich, komputerów, urządzeń mobilnych).
- 2.2. Podłączanie do Zasobów Teleinformatycznych IT lub Systemów OT nieautoryzowanych przez Obszar Bezpieczeństwa IT/OT Nośników Elektronicznych.
- 2.3. Korzystanie z komputerów i urządzeń przenośnych w miejscach publicznych w sposób umożliwiający podgląd aktualnie wyświetlanych Danych na ekranie urządzenia przez osoby nieuprawnione.
- 2.4. Umożliwianie dostępu do Danych przechowywanych w urządzeniach przenośnych lub Nośnikach Elektronicznych osobom nieuprawnionym.
- 2.5. Wykorzystywanie oprogramowania, które nie jest formalnie zatwierdzone przez Obszar Informatyki (zgodnie z zapisami PBTI).

3. Internet

- 3.1. Przetwarzanie Danych poza systemami ORLEN bez akceptacji Dyrektora Wykonawczego ds. Informatyki, w tzw. „Chmurze” (ang. Cloud Computing), to jest w systemach typu „erom”, „virtual-room”, „platformy mobilne”, itp.
- 3.2. Uruchamianie aplikacji, otwieranie plików lub wykorzystywanie odnośników, pozostających bez związku z wykonywaniem obowiązków służbowych, niezależnie, z jakiego źródła zostały pozyskane (od osób znanych lub z niewiadomego źródła).
- 3.3. Udostępnianie w sieci Internet, np. na serwisach społecznościowych, szczegółowych Danych lub informacji dotyczących wykonywanej pracy, w szczególności dotyczących Zasobów Teleinformatycznych IT lub Systemów OT ORLEN, ich konfiguracji, sposobu zabezpieczania, itp.
- 3.4. Tłumaczenia dokumentów wewnętrznych, korespondencji, itp. w całości lub ich fragmentów z wykorzystaniem dostępnych w Internecie translatorów.

4. Poczta elektroniczna

- 4.1. Wykorzystywanie prywatnych skrzynek pocztowych znajdujących się poza domeną pocztową ORLEN do przetwarzania Danych związanych z wykonywanymi obowiązkami służbowymi.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	18 / 40

- 4.2. Podoszywanie się pod innego nadawcę wiadomości poczty elektronicznej lub ukrywanie własnej tożsamości.
- 4.3. Wykorzystywanie nieautoryzowanych klientów poczty elektronicznej i protokołów komunikacyjnych, różnych od stanowiących integralną część konfiguracji oprogramowania (zgodnych z Korporacyjnym Standardem Informatycznym (KSI) na służbowym komputerze lub innym urządzeniu służącym do dostępu do poczty.
- 4.4. Przesyłanie wiadomości poczty elektronicznej o treści lub o zawartości nielegalnej, obraźliwej lub szkodliwej.
- 4.5. Wysyłanie niechcianych przez odbiorcę wiadomości poczty elektronicznej, w tym rozsyłanie wiadomości typu Spam.
- 4.6. Przesyłanie wiadomości poczty elektronicznej niezwiązanych z obowiązkami służbowymi do dużej liczby odbiorców.
- 4.7. Przesyłanie wiadomości poczty elektronicznej do dużej liczby odbiorców, jednocześnie lub w krótkim czasie, o treściach agitacyjnych lub nawołujących do określonych działań, sprzecznych z interesami lub etyką ORLEN i niezgodzonych z właściwą komórką organizacyjną ORLEN.
- 4.8. Przesyłanie Danych związanych z wykonywanymi obowiązkami służbowymi na prywatne konta poczty elektronicznej.
- 4.9. Automatyczne przekazywanie wiadomości poczty elektronicznej poza domenę pocztową ORLEN.
- 4.10. Celowe usuwanie Danych zawartych m.in. w wiadomościach poczty elektronicznej.
- 4.11. Nieuprawnione przekazywanie list adresów poczty elektronicznej z domeny ORLEN osobom nieupoważnionym.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	19 / 40

CYBERBEZPIECZEŃSTWO OT - SYSTEMY OT

UŻYTKOWNICY SYSTEMÓW OT

I. Systemy OT - podstawowe zasady

1. Sterowanie urządzeniami poprzez Systemy OT powinno być nadzorowane i wykonywane przez autoryzowanych do tego Użytkowników OT.
2. Modernizacje lub wdrożenia Systemów OT muszą być realizowane za zgodą i pod nadzorem Inżynierów OT oraz Obszaru Cyberbezpieczeństwa (IT/OT).
3. Dostęp do Systemu OT musi być nadawany, konfigurowany lub usuwany jedynie po akceptacji Inżyniera OT.
4. Dostęp do Systemów OT powinni posiadać tylko Użytkownicy OT, których zakres obowiązków wymaga takiego dostępu. Prawa dostępu powinny być nadawane formalnie i powinny być udokumentowane.
5. Użytkownik OT może używać jedynie precyzyjnie określonych kont w celu logowania do Systemów OT.
6. Użytkownik OT może się logować jedynie do zasobów Systemu OT, które są niezbędne do wykonywania obowiązków służbowych.
7. Użytkownik OT nie powinien logować się do BIOS.
8. Użytkownik OT nie może dokonywać żadnych zmian konfiguracyjnych w systemie operacyjnym.
9. Podłączanie innych zasobów niż komponenty danego Systemu OT do sieci tego Systemu OT jest zabronione.

II. Ochrona przed szkodliwym oprogramowaniem

1. Użytkownik bez zgody Obszaru Cyberbezpieczeństwa (IT/OT) nie może deaktywować oprogramowania antywirusowego ani antymalware.
2. Użytkownik w przypadku stwierdzenia braku oprogramowania antywirusowego lub jego nieprawidłowego działania (w zakresie, jakim użytkownik może to wykonać) – fakt ten musi zgłosić do HelpDesk.

III. Instalowanie/odinstalowywanie oraz uruchamianie/wyłączanie oprogramowania

1. Użytkownik OT nie jest uprawniony do instalowania lub usuwania żadnego oprogramowania w Systemach OT.
2. W przypadku zaistnienia potrzeby, instalacja oprogramowania jest wykonywana przez Inżyniera OT i zgodnie z obowiązującymi zasadami w tym zakresie.
3. Użytkownik OT nie może uruchamiać w Systemie OT oprogramowania innego niż jest dopuszczone do eksploatacji na danym Systemie OT, zainstalowane jak również wymagane do wypełniania obowiązków służbowych.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	20 / 40

IV. Sieci teleinformatyczne

1. Dostęp do sieci Internet z Systemów OT lub dowolnego komponentu podłączonego do sieci Systemów OT jest zabroniony.
2. Bezpośredni dostęp do Systemów OT z sieci Internet jest zabroniony.
3. Dostęp do Systemu OT spoza sieci Systemów OT (z wyłączeniem sieci Internet) powinien być możliwy wyłącznie dla autoryzowanych usług i Użytkowników OT z wykorzystaniem autoryzowanych protokołów i środków uwierzytelniających. Autoryzacji może dokonać jedynie Obszar Cyberbezpieczeństwa (IT/OT).
4. Użytkownicy nie mogą podłączać komponentów Systemów OT do sieci teleinformatycznych IT.
5. Użytkownicy nie mogą podłączać dowolnych zasobów teleinformatycznych do sieci Systemów OT.

V. Poczta elektroniczna

1. Korzystanie przez Użytkownika z poczty elektronicznej poprzez zasoby Systemów OT lub poprzez dowolne elementy podłączone do sieci Systemów OT jest zabronione.

VI. Nośniki Elektroniczne

1. Użytkownik OT nie może podłączać do Systemu OT nośników zewnętrznych (np. pamięci masowych USB, płyt CD/DVD).

VII. Zarządzanie zmianą

1. Zmiany w zakresie konfiguracyjnym komponentów oraz funkcjonalności Systemów OT mających wpływ na cyberbezpieczeństwo teleinformatyczne muszą być dokonywane jedynie po akceptacji Inżyniera OT oraz Obszaru Cyberbezpieczeństwa (IT/OT).
2. Zmiany w zakresie konfiguracji cyberbezpieczeństwa w Systemach OT muszą być dokonywane po akceptacji Obszaru Bezpieczeństwa (IT/OT).

INŻYNIEROWIE SYSTEMÓW OT

I. Zarządzanie dostępem do Systemów OT

Identyfikacja użytkowników

1. Identyfikacja, a następnie uwierzytelnianie jest pierwszą, prewencyjną linią obrony w Systemach OT przed dostępem osób nieuprawnionych, dlatego też każdy użytkownik powinien posiadać jednoznacznie przypisany identyfikator (login) wyłącznie do swojego osobistego użytku, tam gdzie jest to technicznie możliwe. Odstępstwo od niniejszej reguły wymaga akceptacji Kierownika Inżynierów OT oraz Obszaru Cyberbezpieczeństwa (IT/OT).
2. Nazwy Użytkowników OT w Systemach OT nadawane są po akceptacji Inżyniera OT. Nazwy Użytkowników OT należy nadawać zgodnie z przyjętą konwencją nazewnictwa, która umożliwia jednoznaczną identyfikację Użytkownika OT (np. nazwisko i pierwsza litera imienia).

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	21 / 40

3. W Systemach OT działania realizowane przez Użytkowników OT muszą być rozliczane i być jednoznacznie przypisane do danego Użytkownika OT uwzględniając odstępstwa opisane w punkcie 1.
4. Każde konto funkcyjne (grupowe) lub serwisowe musi być odpowiednio oznaczone i udokumentowane.
5. Elementy identyfikujące Użytkownika OT (np. tzw. identyfikator lub login), któremu odebrany został dostęp do Systemu OT, nie mogą zostać powtórnie wykorzystane przez inną osobę.
6. Konta Użytkowników OT, którzy nie są etatowymi pracownikami Spółki, muszą być odpowiednio oznaczone, umożliwiając w łatwy sposób odróżnienie ich od kont pracowników Spółki.
7. Konta typu „gość” standardowo zaimplementowane w Systemach OT powinny być usunięte lub zablokowane.
8. Domyślne konta dostępowe powinny zostać wyłączone, jeśli jest to technicznie możliwe.
9. Wszystkie domyślne hasła dostępowe powinny być zmienione.

Uwierzytelnienie

1. Uwierzytelnienie w Systemach OT powinno następować po identyfikacji Użytkownika OT, czyli po zadeklarowaniu swojej tożsamości (np. przez podanie loginu). Zadeklarowana, ale jeszcze niezweryfikowana tożsamość jest potwierdzana w procesie uwierzytelnienia (np. przez podanie hasła, PIN).
2. Użytkowników OT należy uwierzytelniać za pomocą odpowiednich metod uwierzytelniania, którymi mogą być:
 - 2.1. Hasła statyczne – „coś, co wiesz”, sekwencje liter, cyfr i innych znaków, mechanizm najłatwiejszy w użyciu z punktu widzenia Użytkownika.
 - 2.2. Hasła jednorazowe - (ang. One Time Password), „coś, co masz”, hasło jednorazowe jest wykorzystywane tylko raz i traci ważność po wykorzystaniu lub po upływie określonego czasu ważności.
 - 2.3. Certyfikaty – uwierzytelnianie oparte o dowód posiadania klucza prywatnego z użyciem kryptografii asymetrycznej.
 - 2.4. Dwuskładnikowe – (ang. two-factor authentication) jest kombinacją opisanych powyżej metod uwierzytelniania np. wykorzystanie tego, co wiesz (np. hasło, PIN) wraz z wykorzystaniem tego, co masz (np. certyfikat, hasło jednorazowe, token/klucz).
3. Elementy mechanizmów uwierzytelniających Użytkowników OT muszą być chronione przed nieautoryzowanym dostępem zarówno po stronie Użytkowników OT, jak i po stronie Systemów OT.
4. Za zapewnienie narzędzi do bezpiecznego przechowywania haseł odpowiada Obszar Cyberbezpieczeństwa (IT/OT).

Zarządzanie uprawnieniami

1. Uprawnienia przyznawane Użytkownikom OT muszą być nadawane z uwzględnieniem rozdziału odpowiedzialności i zakresu obowiązków służbowych.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	22 / 40

2. Użytkownik OT nie może posiadać uprawnień administratorskich lub innych uprawnień umożliwiających instalacje/odinstalowywanie oprogramowania, dokonywanie zmian konfiguracyjnych w Systemach OT.
3. Bezpośredni dostęp do konsoli poleceń systemów operacyjnych, serwerów aplikacji, serwerów baz danych, aktywnych urządzeń sieciowych oraz urządzeń automatyki przemysłowej (z wykorzystaniem uprzywilejowanych kont) może być dozwolony po akceptacji Inżyniera OT i Obszaru Cyberbezpieczeństwa (IT/OT).
4. Konta dostępowe dla Inżynierów Firm Zewnętrznych (OT) powinny być jedynie odblokowywane przez Inżyniera OT na czas bezpośredniego wykonywania prac w Systemach OT.
5. Dostęp do rozwiązań i narzędzi cyberbezpieczeństwa powinien być ograniczany wyłącznie dla Obszaru Cyberbezpieczeństwa (IT/OT), wszelkie odstępstwa muszą być akceptowane przez Obszar Cyberbezpieczeństwa (IT/OT).

Zarządzanie dostępem Użytkowników OT

1. Podstawowe założenie dotyczące zarządzania dostępem Użytkowników OT zakłada, że wszelki dostęp do Systemów OT jest zabroniony z wyjątkiem tego, który został wyraźnie określony jako dozwolony.
2. Systemy OT powinny być wyposażone w środki zapewniające odpowiedni poziom Bezpieczeństwa Teleinformatycznego / Cyberbezpieczeństwa (np. kontrolę dostępu, minimalizację wpływu szkodliwego oprogramowania).
3. Za zarządzanie dostępem do Systemu OT odpowiada Inżynier OT.
4. Za separację sieci systemów OT od sieci korporacyjnej odpowiada Obszar Cyberbezpieczeństwa (IT/OT), za fizyczną realizację separacji w zakresie urządzeń sieciowych odpowiada Dział Sieci Teleinformatycznych.

Zarządzanie dostępem Stron Trzecich

1. Dostęp Stron Trzecich do Systemów OT powinien być przeanalizowany pod kątem bezpieczeństwa. Korzyści związane z dostępem Stron Trzecich muszą uwzględniać ryzyka związane z takim dostępem.
2. Strony Trzecie mogą uzyskać dostęp do Systemów OT wyłącznie po podpisaniu stosownego porozumienia ze Spółką, w którym zostaną określone zasady dostępu, zakres i okres dostępu oraz niezbędne wymagania Bezpieczeństwa Teleinformatycznego / Cyberbezpieczeństwa.
3. W zawieranych ze Stronami Trzecimi umowach na świadczenie usług muszą być uwzględnione co najmniej następujące elementy: precyzyjna definicja usług, wymagane środki bezpieczeństwa organizacyjnego i technicznego po stronie dostawcy usług, oczekiwany poziom usług, konieczność podpisania przez Strony Trzecie oświadczeń o zachowaniu poufności, zasady współpracy w przypadku incydentów związanych z bezpieczeństwem oraz mechanizmy pozwalające na kontrolę i wgląd we wszystkie aspekty związane z bezpieczeństwem.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	23 / 40

4. Każda umowa przewidująca dostęp Stron Trzecich do Systemów OT musi być przekazana, w trybie określonym w odrębnym wewnętrznym akcie organizacyjnym, do opiniowania i akceptacji Obszaru Cyberbezpieczeństwa (IT/OT).
5. Zakres dostępu Stron Trzecich do Systemów OT powinien ograniczać się wyłącznie do tych zasobów, do których dostęp jest niezbędny w celu realizacji umowy lub porozumienia i który został określony w umowie lub w porozumieniu.
6. W umowach lub porozumieniach, w części poświęconej dostępowi Stron Trzecich do Systemów OT, należy zawrzeć prawo do kontroli przez Spółkę sposobów realizacji spełnienia wymagań Bezpieczeństwa Teleinformatycznego wynikających z PBTi i określonych w treści rzeczowej umowy lub porozumienia.
7. Spełnienie określonych w umowie lub w porozumieniu wymagań Bezpieczeństwa Teleinformatycznego, zaakceptowanych przez Obszar Informatyki powinno być pisemnie potwierdzone przez przedstawiciela Strony Trzeciej przed uzyskaniem dostępu do Systemów OT.
8. Dla każdej Strony Trzeciej, która będzie miała dostęp do Systemów OT należy wyznaczyć po stronie Spółki osobę (np. właściciel merytoryczny umowy) odpowiedzialną za realizację umowy lub porozumienia. Na osobie tej spoczywa odpowiedzialność za wypełnienie zobowiązań Strony Trzeciej, o których mowa w PBTi.
9. Strony Trzecie przed uzyskaniem dostępu do Systemów OT muszą zapoznać się z zasadami bezpieczeństwa teleinformatycznego określonymi w niniejszej Polityce. Odpowiedzialność za dopełnienie tego obowiązku leży po stronie osoby odpowiedzialnej za realizację umowy lub porozumienia ze strony Spółki.
10. Przedłużanie okresu ważności dostępu może być realizowane wyłącznie w związku z ważnym procesem biznesowym oraz po zaktualizowaniu umowy lub porozumienia i musi być każdorazowo zatwierdzane przez Obszar Cyberbezpieczeństwa.
11. Usługi świadczone przez Strony Trzecie muszą podlegać monitorowaniu i przeglądom w celu weryfikacji zgodności z zapisami zawartymi w umowach na świadczenie usług.

Konta uprzywilejowane

1. Wszystkie konta uprzywilejowane w Systemach OT muszą być identyfikowalne.
2. Podczas wykonywania czynności niewymagających użycia uprzywilejowanych kont zabrania się ich stosowania.
3. Czynności wykonywane w systemach operacyjnych za pomocą kont uprzywilejowanych należy rejestrować oraz zapewnić możliwość ich identyfikacji i rozliczalności.
4. Czynności związane z nadużywaniem poziomów dostępu, w tym uprawnień uprzywilejowanych mogą skutkować co najmniej utratą tych uprawnień.
5. Uprawnienia do kont uprzywilejowanych w Systemach OT, z wyłączeniem Inżynierów OT, nadawane są po akceptacji Inżyniera OT i Obszaru Cyberbezpieczeństwa (IT/OT)
6. Hasła do kont uprzywilejowanych muszą być przechowywane w elektronicznym sejfie Spółki.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	24 / 40

Konta funkcyjne i serwisowe

1. Wykorzystywanie kont funkcyjnych (grupowych) jest dozwolone wyłącznie, gdy uzasadniają to ważne potrzeby biznesowe i nie ma innego sposobu zapewnienia dostępu do Systemów OT, a ich stosowanie powinno być udokumentowane oraz zatwierdzone przez Obszar Cyberbezpieczeństwa.
2. W przypadku wykorzystywania kont funkcyjnych, a co za tym idzie również haseł do nich przypisanych, należy zapewnić organizacyjne oraz techniczne środki zapewniające rozliczalność wykorzystywanych kont grupowych, które zapewnią w sposób jednoznaczny identyfikację kto i kiedy korzystał z tego konta.
3. Konta serwisowe nie powinny mieć włączonej możliwości logowania interakcyjnego i powinny być wykorzystywane wyłącznie zgodnie z przeznaczeniem, to jest np. do działania skryptów lub usług.

II. Zabezpieczenia kryptograficzne

1. Zabezpieczenia kryptograficzne powinny być stosowane w każdym przypadku wymaganym przez przepisy wewnętrzne, przepisy prawa lub zobowiązania kontrahentów.
2. Wymagania stosowania zabezpieczeń kryptograficznych dotyczą Użytkowników OT.
3. W przypadku stosowania infrastruktury klucza publicznego (PKI) w Systemach OT, certyfikaty muszą być wystawiane przez wewnętrzne urzędy certyfikacyjne Spółki.
4. Klucze kryptograficzne, wygenerowane przez pracowników Spółki w celach służbowych, są własnością Spółki i muszą być należycie chronione przed ujawnieniem osobom nieuprawnionym.
5. Klucze kryptograficzne muszą być zabezpieczone przed nieautoryzowanym użyciem, ujawnieniem, modyfikacją lub zniszczeniem.
6. Klucze kryptograficzne powinny być generowane oraz przechowywane z zachowaniem należytego bezpieczeństwa, w bezpiecznych urządzeniach lub środowiskach odpowiednich do tego celu. Dla bezpiecznego zarządzania kluczami kryptograficznymi zalecane jest wykorzystywanie sprzętowych modułów bezpieczeństwa (HSM).
7. Należy zapewnić, aby parametry techniczne kluczy (algorytm, długość klucza, funkcja skrótu) wykorzystywanych produkcyjnie spełniały ogólnie uznane wymagania dotyczące bezpieczeństwa (źródłem odniesienia mogą być np. publikacje NIST ang. National Institute of Standards and Technology). Dotyczy to zarówno nowo generowanego materiału kryptograficznego, jak i aktualnie wykorzystywanego (konieczność aktualizacji w przypadku nie spełnienia przywołanych wymagań). W przypadku podejrzenia ujawnienia osobom nieuprawnionym, materiał kryptograficzny musi być wygenerowany powtórnie i zmieniony na urządzeniach go wykorzystujących. W przypadku kryptografii asymetrycznej, certyfikaty powiązane z kluczem prywatnym, do którego dostęp miały osoby nieautoryzowane, muszą być unieważnione.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	25 / 40

III. Zasoby Systemów OT

Ochrona przed szkodliwym oprogramowaniem

1. Ochrona przed szkodliwym oprogramowaniem, którego celem jest szkodliwe, przestępcze lub złośliwe działanie w stosunku do Systemów OT, powinna być ukierunkowana na niezwłoczne wykrywanie, usuwanie bądź blokowanie szkodliwego oprogramowania.
2. W celu uniknięcia destrukcyjnych oraz kosztownych implikacji, jakie mogą być wywołane działaniem szkodliwego oprogramowania, ochrona antywirusowa oraz antymalware musi być zgodna z zasadami określonymi w niniejszej Polityce oraz standardami i zaleceniami Obszaru Cyberbezpieczeństwa (IT/OT).
3. Zarządzanie ochroną antywirusową oraz ochroną antymalware musi spełniać wymagania bezpieczeństwa z naciskiem na takie aspekty, jak: dostępność integralność, oraz poufność.
4. Zastosowanie zabezpieczenia ochrony antywirusowej oraz ochrony antymalware powinny być adekwatne dla danego Systemu OT i uwzględniać aspekty techniczne Systemu OT.
5. Ochrona antywirusowa oraz ochrona antymalware swoim obszarem powinna obejmować, wszystkie komponenty Systemów OT, które technicznie i organizacyjnie umożliwiają stosowanie takich zabezpieczeń.
6. Oprogramowanie antywirusowe oraz oprogramowanie antymalware użyte do ochrony Systemów OT musi być odpowiednio skonfigurowane, aby chronić je przed zagrożeniami ze strony szkodliwego oprogramowania, a jednocześnie, aby nie powodowało komplikacji w prawidłowym działaniu Systemów OT.
7. Oprogramowanie antywirusowe oraz oprogramowanie antymalware użyte do ochrony Systemów OT powinno być przetestowane uwzględniając aspekty prawidłowego działania Systemów OT.
8. Oprogramowanie antywirusowe oraz oprogramowanie antymalware powinno posiadać najnowsze i przetestowane dla danego Systemu OT sygnatury.
9. Oprogramowanie antywirusowe jest jednym z kluczowych elementów każdej koncepcji Bezpieczeństwa Teleinformatycznego i powinno:
 - 9.1. Reprezentować najnowsze dostępne, przetestowane metody obrony przed zagrożeniami.
 - 9.2. Chronić przed zagrożeniami.
 - 9.3. Posiadać wbudowane mechanizmy natychmiastowej reakcji przeciwko atakom ze strony szkodliwego oprogramowania.
 - 9.4. Posiadać automatyczną aktualizację bazy sygnatur np. poprzez dystrybucję z serwera zarządzającego. W przypadku braku takiej możliwości, aktualizacja powinna być prowadzona manualnie, co najmniej raz na miesiąc. Za prawidłowy przebieg powyższych czynności odpowiada Inżynier OT.
 - 9.5. zapewnienie infrastruktury informatycznej do pobierania sygnatur odpowiada Obszar Cyberbezpieczeństwa (IT/OT).
10. Systemy operacyjne i antywirusowe powinny być tak skonfigurowane, aby Użytkownicy OT nie mogli zmieniać konfiguracji lub usuwać systemów antywirusowych ze stacji roboczych.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	26 / 40

Instalowanie/odinstalowywanie oraz uruchamianie/wyłączanie oprogramowania

1. Instalowanie/odinstalowywanie, uruchamianie/wyłączanie oprogramowania w Systemach OT w zakresie utrzymania ciągłości działania Systemu OT mogą inicjować tylko Inżynierowie OT.
2. Proces instalowania/odinstalowywania oraz uruchamiania/wyłączania oprogramowania w Systemach OT w zakresie cyberbezpieczeństwa Systemu OT może być inicjowany po akceptacji Obszaru Cyberbezpieczeństwa (IT/OT).
3. Instalowanie / odinstalowywanie, uruchamianie / wyłączanie oprogramowania w Systemach OT powinno uwzględniać aspekty prawidłowego, ciągłego działania Systemów OT.
4. Każde instalowanie / odinstalowywanie oraz uruchamianie / wyłączanie oprogramowania w Systemach OT powinno być zgodne z PBTi oraz prowadzone według procedury adekwatnej dla danego oprogramowania i Systemu OT.
5. Każde instalowane/uruchamiane oraz używane oprogramowanie w Systemach OT musi mieć aktualną licencję uprawniającą do jego instalacji/uruchomienia oraz używania w środowisku, w którym jest to wykonywane oraz musi pochodzić z zaufanego źródła.

Nośniki Elektroniczne

1. Konfiguracja Systemów OT powinna uniemożliwić podłączenie przez nieautoryzowane osoby Nośników Elektronicznych do zasobów Systemów OT.
2. Konfiguracja Systemów OT powinna umożliwić elektroniczną rejestrację każdego faktu podłączenia/użycia Nośnika Elektronicznego.
3. Do systemów OT można jedynie podłączać Nośniki Elektroniczne dedykowane do Systemów OT i zatwierdzone przez Obszar Cyberbezpieczeństwa (IT/OT). Niedozwolone jest podłączanie do Systemów OT Nośników Elektronicznych niezaakceptowanych przez Obszar Cyberbezpieczeństwa (IT/OT).
4. Wszystkie Nośniki Elektroniczne dedykowane do Systemów OT powinny być zinwentaryzowane przez Kierownika Utrzymania OT i przechowywane w sposób ograniczający dostęp osób nieuprawnionych.
5. Nośniki Elektroniczne zatwierdzone przez Obszar Cyberbezpieczeństwa (IT/OT) do podłączenia do Systemów OT nie mogą być stosowane do podłączania do innych zasobów niż Systemy OT oraz służbowe stacje robocze danego Inżyniera OT.
6. Każdorazowo przed wykorzystaniem Nośnika Elektronicznego należy wykonać jego skanowanie z wykorzystaniem systemu antywirusowego.
7. Nośniki Elektroniczne zatwierdzone przez Obszar Cyberbezpieczeństwa (IT/OT) do podłączenia do Systemów OT powinny być wykorzystywane wyłącznie w zakresie, który jest niezbędny do wykonywania obowiązków służbowych wynikających z obsługi Systemów OT.
8. Dane przechowywane na Nośnikach Elektronicznych dotyczące Systemów OT powinny być odpowiednio zaszyfrowane.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	27 / 40

- Incydenty związane z Nośnikami Elektronicznymi (np. infekcja, kradzież, zagubienie) przeznaczonymi do Systemów OT należy niezwłocznie zgłaszać do HelpDesk.

Urządzenia mobilne w obszarze Systemów OT

- Urządzenia Mobilne OT wykorzystywane w Systemach OT muszą być autoryzowane przez Obszar Cyberbezpieczeństwa (IT/OT).
- Urządzenia Mobilne OT wykorzystywane w Systemach OT muszą mieć aktywną ochronę antywirusową wraz z najnowszą bazą wirusów, a zainstalowany system operacyjny powinien być wspierany przez producenta oraz zaktualizowany.
- Urządzenia Mobilne OT powinny być zabezpieczone przed nieautoryzowanym zalogowaniem się.
- Do korzystania z Urządzeń Mobilnych OT w Systemach OT autoryzowani są jedynie Inżynierowie OT.
- Inżynierowie OT są odpowiedzialni za konfigurację i używanie Urządzeń Mobilnych zgodnie z PBTI.
- Wszystkie Urządzenia Mobilne OT powinny być zinwentaryzowane przez Kierownika Utrzymania OT i przechowywane w sposób ograniczający dostęp osób nieuprawnionych.
- Każde użycie Urządzenia Mobilnego OT w Systemach OT powinno być rejestrowane i ewidencjonowane wraz z informacjami, jaki użytkownik oraz w jakim czasie korzystał z Urządzenia Mobilnego OT.
- Obszar Cyberbezpieczeństwa (IT/OT) jest uprawniony do przeprowadzania przeglądów Urządzeń Mobilnych OT.

Polityki i bezpieczeństwo kopii zapasowych

- Realizacja procesów związanych z wykonywaniem kopii zapasowych nie może ograniczać funkcjonowania Systemów OT.
- Sposób, zakres oraz częstotliwość tworzenia kopii zapasowych Systemów OT powinny odzwierciedlać wymagania biznesowe, wymagania bezpieczeństwa, wymagania prawa powszechnie obowiązującego oraz stopień krytyczności przetwarzanych Danych.
- Wybór nośników do przechowywania kopii zapasowych i archiwalnych Systemów OT powinien być podyktowany wymaganiami biznesowymi (w szczególności w zakresie bezpieczeństwa danych), jak również ich parametrami takimi jak czas odtwarzania danych, długość możliwego okresu przechowywania i odporność na uszkodzenia. Zalecane jest przechowywanie kopii zapasowych na zasobach zapewnionych przez Obszar IT.
- Za proces wykonania kopii zapasowej i archiwalnej odpowiada Inżynier OT.
- Weryfikację poprawności wykonywania kopii zapasowych i archiwalnych Systemów OT należy przeprowadzać np. podczas odbiorów fabrycznych systemów.
- Urządzenia służące do wykonywania kopii zapasowych powinny być odpowiednio utrzymywane i konserwowane, zgodnie z zaleceniami producenta.
- Nośniki kopii zapasowych i archiwalnych powinny być eksploatowane w taki sposób, aby umożliwić ich jak najdłuższą bezawaryjną pracę.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	28 / 40

8. W przypadku wystąpienia błędów w trakcie wykonywania kopii zapasowej bądź archiwalnej, za ich przeanalizowanie oraz podjęcie działań mających na celu niezwłoczne usunięcie ich przyczyn oraz ponowne wykonanie kopii odpowiada Inżynier OT.
9. Kopie zapasowe należy odpowiednio chronić przed nieuprawnionym dostępem, nadużyciem lub uszkodzeniem poprzez zastosowanie odpowiednich zabezpieczeń organizacyjnych i technicznych, zgodnych z wymaganiami prawa powszechnie obowiązującego, wymaganiami obowiązujących regulacji wewnętrznych oraz uznanymi międzynarodowymi standardami.
10. Dostęp do kopii zapasowych powinien być zgodny z nadanymi i autoryzowanymi uprawnieniami.
11. Nośniki, na których są przechowywane kopie zapasowe należy odpowiednio przechowywać z dala np. od działania ciepła, czynników szkodliwych dla zapisanych Danych oraz zgodnie z zaleceniami producenta.
12. Urządzenia wykorzystywane do wykonywania kopii zapasowych muszą być poddawane okresowym czynnościom konserwacyjnym w celu zapewnienia ich odpowiedniego funkcjonowania.

IV. Model planowania, wdrożenia, utrzymania i rozwoju Systemów OT

Rozdzielenie środowisk

1. Środowiska o charakterze testowym i rozwojowym muszą być fizycznie rozdzielone od środowisk produkcyjnych i nie mogą w środowiskach testowych lub rozwojowych być przetwarzane Dane produkcyjne.
2. W przypadku, gdy rozdzielenie środowisk testowych/rozwojowych od środowisk produkcyjnych jest niemożliwe lub nieuzasadnione ekonomicznie dopuszczalne jest, za zgodą odpowiedniego Kierownika Utrzymania OT, czasowe prowadzenie prac rozwojowych w środowisku produkcyjnym. Każdorazowo, odstępstwo takie należy udokumentować oraz poddać dodatkowej kontroli Obszaru Cyberbezpieczeństwa (IT/OT).
3. Dostęp do środowisk produkcyjnych należy ograniczyć wyłącznie do uprawnionych Użytkowników. Dostęp do środowisk produkcyjnych Systemów OT dla Inżynierów Firm Zewnętrznych (OT) w zakresie funkcjonalności i komponentów Systemów OT może być przyznany wyłącznie za zgodą odpowiedniego Kierownika Utrzymania OT, zaś w zakresie cyberbezpieczeństwa za zgodą Obszaru Bezpieczeństwa (IT/OT).

Aspekty cyberbezpieczeństwa przy projektowaniu Systemów OT

1. W trakcie projektowania Systemów OT należy mieć na uwadze, że środki zapewniające bezpieczeństwo są znacząco tańsze i bardziej efektywne, jeżeli są wprowadzane w momencie specyfikacji wymagań i na etapie projektowania.
2. Wymagania w zakresie cyberbezpieczeństwa, jakim podlegają Systemy OT, wynikają ze standardów cyberbezpieczeństwa oraz zidentyfikowanego ryzyka i powinny być zdefiniowane przez Obszar Cyberbezpieczeństwa. W procesie definiowania wymagań bezpieczeństwa należy uwzględnić m.in.:

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	29 / 40

- 2.1. Przepisy prawne, regulacje wewnętrzne ORLEN i standardy, jakim podlegają Systemy OT, w tym „Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS – OT”.
- 2.2. Przeznaczenie Systemu OT oraz sposoby jego wykorzystania przez przyszłych Użytkowników OT.
- 2.3. Przewidywane nowe zagrożenia dla bezpieczeństwa teleinformatycznego, jakie mogą się pojawić w związku z rozpoczęciem eksploatacji danej aplikacji.
- 2.4. Rodzaje przetwarzanych danych.
- 2.5. Mechanizmy identyfikacji, uwierzytelniania i autoryzacji.
- 2.6. Infrastrukturę teleinformatyczną.
- 2.7. Wymagania dotyczące logowania zdarzeń systemowych i aktywności Użytkownika OT.
3. Wymagania w zakresie bezpieczeństwa, jakim mają podlegać Systemy OT, należy przekazać osobom odpowiedzialnym za projektowanie i upewnić się, że wszystkie wymagania zostały zrozumiane i będą uwzględnione.
4. W przypadku rozbudowanych Systemów OT, mających wspierać krytyczne procesy biznesowe, należy rozważyć podział na moduły, posiadające niezależne mechanizmy bezpieczeństwa.
5. W celu zapewnienia możliwie najwyższego poziomu bezpieczeństwa Systemów OT, należy w procesie projektowania wykorzystać sprawdzone standardy i dobre praktyki w tym obszarze.

Aspekty cyberbezpieczeństwa w fazie wdrażania Systemów OT

1. Przed rozpoczęciem wdrożenia Systemu OT należy opracować szczegółową dokumentację zawierającą opis wymagań funkcjonalnych i poza-funkcjonalnych, uwzględniającą standard „Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS – OT oraz dodatkowe wymagania zatwierdzone przez Obszar Cyberbezpieczeństwa.
2. Proces wdrażania Systemu OT może się rozpocząć dopiero w momencie zatwierdzenia projektu przez Obszar Cyberbezpieczeństwa.
3. Na etapie wdrożenia Systemu OT wszystkie aspekty związane z cyberbezpieczeństwem podlegają akceptacji Obszaru Cyberbezpieczeństwa (IT/OT).
4. W celu zapewnienia możliwie najwyższego poziomu bezpieczeństwa Systemów OT, należy w procesie wdrożenia wykorzystać sprawdzone standardy i dobre praktyki w tym obszarze.
5. W przypadku wystąpienia konieczności uwzględnienia niezdefiniowanych przed rozpoczęciem procesu wdrożenia wymagań bezpieczeństwa, należy dokonać szczegółowej analizy już wykonanych prac pod kątem możliwości implementacji dodatkowych wymagań.
6. Przed produkcyjnym uruchomieniem Systemu OT należy upewnić się, że mający z niej korzystać Użytkownicy OT posiadają odpowiednie umiejętności do posługiwania się Systemem OT.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	30 / 40

Testowanie cyberbezpieczeństwa Systemów OT

1. Przed przystąpieniem do procesu testowania cyberbezpieczeństwa Systemów OT wymagane jest opracowanie planu testów cyberbezpieczeństwa.
2. Plan testów cyberbezpieczeństwa Systemu OT (oraz obejmujący go ogólny plan wdrożenia w ORLEN) powinien uwzględniać możliwość wykrycia błędów i wynikających z tego opóźnień.
3. Testy akceptacyjne cyberbezpieczeństwa Systemu OT powinny w możliwie jak największym stopniu odzwierciedlać rzeczywiste warunki eksploatacji.
4. W przypadku identyfikacji błędów podczas testów cyberbezpieczeństwa Systemów OT, po wprowadzeniu odpowiednich poprawek, testy należy powtórzyć w pełnym ich zakresie lub w zakresie obejmującym elementy, w których wprowadzono poprawki.
5. Wyniki testów akceptacyjnych cyberbezpieczeństwa Systemów OT należy odpowiednio udokumentować oraz poddać analizie zgodności z wymaganiami.
6. Odbiory Systemu OT mogą się odbyć jedynie po zatwierdzeniu przez uprawnioną osobę wyników testów akceptacyjnych cyberbezpieczeństwa.

Odbiór Systemów OT

1. Kryteria końcowego odbioru Systemu OT należy odpowiednio zdefiniować i udokumentować.
2. Warunkiem koniecznym do odbiór Systemu OT jest pozytywny wynik testów akceptacyjnych cyberbezpieczeństwa.
3. Obszar Cyberbezpieczeństwa przekazuje do Komisji odbiorowych oświadczenie dotyczące cyberbezpieczeństwa Systemów OT.

v.Sieć OT

Zasady dotyczące korzystania z usług sieci OT

1. Użytkownikom należy zapewnić dostęp tylko do tych usług infrastruktury Systemów OT, do których posiadają uprawnienia.
2. Obszar Cyberbezpieczeństwa (IT/OT) określa zasady, weryfikuje i monitoruje separację sieci IT/OT.
3. Należy zapewnić, że niezabezpieczone usługi infrastruktury Systemów OT, pozwalające przysyłać hasła w postaci niezabezpieczonej np. telnet lub ftp, nie są wykorzystywane i są zablokowane.

Podstawowa ochrona sieci

1. Właściwa ochrona sieci powinna być zapewniona poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, adekwatnych do występujących podatności oraz na odpowiednim poziomie technicznym.
2. Samodzielne lub nieuprawnione podłączanie do sieci Systemów OT ORLEN prywatnych urządzeń pracowników i urządzeń Inżynierów Firm Zewnętrznych (OT) (np. audytorzy,

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	31 / 40

konsultanci) bez uzasadnionej potrzeby biznesowej i zgody uprawnionego przez Kierownika Utrzymania OT lub Inżyniera OT jest zabronione.

3. Zabrania się samodzielnych modyfikacji, ingerencji, zmiany lokalizacji lub podłączeń do sieci Systemów OT bez uzyskania zgody uprawnionego Kierownika Utrzymania OT i/lub Inżyniera OT. Podłączanie we własnym zakresie stacji roboczych do publicznej sieci telekomunikacyjnej poprzez nieautoryzowane urządzenia sieci teleinformatycznych, będąc jednocześnie podłączonym do sieci teleinformatycznej ORLEN jest zabronione.
4. Wewnętrzna adresacja IP, konfiguracja usług sieciowych, topologia, nazwy i modele urządzeń sieci oraz informacja o zasobach powiązanych nie może być ujawniana osobom nieuprawnionym.

Zarządzanie bezpieczeństwem sieci

1. Połączenie poszczególnych elementów infrastruktury Systemów OT do innych sieci nie powinno obniżać poziomu bezpieczeństwa oraz powinno być formalnie uzgodnione i zatwierdzone.
2. W celu zwiększenia poziomu bezpieczeństwa Systemów OT dla poszczególnych obszarów usług Systemów OT należy stosować segmentację sieci.
3. Dostęp konfiguracyjny do urządzeń aktywnych (np. switchy, firewalli, routerów) w sieciach produkcyjnych powinien być ograniczony tylko do autoryzowanych Inżynierów OT.
4. Obszar Cyberbezpieczeństwa określa zasady, weryfikuje i monitoruje separację sieci IT/OT.
5. Powinny być stosowane rozwiązania ukrywające informacje o stosowanych urządzeniach, systemach, aplikacjach i inne informacje, które mogą ułatwić intruzowi potencjalny atak.
6. Konfiguracja urządzeń aktywnych powinna być prowadzona zgodnie z uznaną praktyką w tym zakresie, formalnie dokumentowana oraz okresowo weryfikowana.
7. Kopie zapasowe konfiguracji urządzeń aktywnych powinny być regularnie wykonywane oraz zabezpieczone w sposób zapewniający ich poufność, dostępność i integralność.

Sieci bezprzewodowe

1. Sieć bezprzewodowa Systemów OT jest przeznaczona wyłącznie dla funkcjonowania dedykowanych systemów, których architektura tego wymaga. Wykorzystywanie sieci bezprzewodowej dla innych celów jest zabronione. W tym celu powinny być zaimplementowane odpowiednie metody uwierzytelnienia oraz szyfrowania transmisji danych.
2. Sieć bezprzewodowa Systemów OT powinna być wydzieloną siecią z ograniczonym dostępem.
3. Punkty dostępowe powinny być umieszczone, tak, aby w miarę możliwości uniemożliwić dostęp do sieci bezprzewodowej Systemów OT spoza obszaru ORLEN, w szczególności z obszaru publicznie dostępnego.
4. Próby nieautoryzowanego dostępu do sieci bezprzewodowych Systemów OT powinny być monitorowane, a wykrycie nieautoryzowanych punktów dostępowych dokumentowane i weryfikowane.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	32 / 40

- Przesyłane za pomocą sieci bezprzewodowej Dane powinny podlegać ochronie w celu zapewnienia poufności i integralności poprzez wykorzystanie odpowiednich mechanizmów kryptograficznych.
- W celu utrudnienia nieautoryzowanego dostępu poprzez urządzenie mobilne należy zapewnić wymuszanie uwierzytelnienia użytkownika przed uzyskaniem dostępu do sieci bezprzewodowych.

Zdalny dostęp dla Inżynierów Firm Zewnętrznych (OT)

- Zdalny dostęp do Systemów OT dla Stron Trzecich jest przeznaczony wyłącznie dla świadczenia usług wsparcia w zakresie utrzymania danego Systemu OT na podstawie umowy, zamówienia lub porozumienia.
- W celu realizacji zdalnego połączenia przez Inżynierów Firm Zewnętrznych (OT), wymagane jest zawarcie odpowiednich zapisów w umowach, zamówieniach, porozumieniach regulujących ten fakt, uzyskanie zgody Obszaru Cyberbezpieczeństwa (IT/OT) oraz podpisanie porozumienia odnośnie połączenia zdalnego.
- Zdalny dostęp do Systemów OT powinien odbywać się dwukrotnie, tzn. pierwszym krokiem jest logowanie do sieci korporacyjnej, drugim krokiem jest logowanie do sieci Systemów OT.
- Nawiązanie połączenia zdalnego z Systemami OT może być realizowane wyłącznie za pośrednictwem tzw. serwera przesiadkowego, odpowiednio skonfigurowanego i zarządzanego, pełniącego rolę pośredniego punktu uwierzytelnienia w Systemach OT.
- Komputery nienależące do ORLEN, wykorzystywane do zdalnego dostępu do Systemów OT, muszą zostać skonfigurowane zgodnie z wytycznymi ORLEN w zakresie bezpieczeństwa.
- Wszystkie połączenia zdalne, w tym te z Systemami OT, jak również próby nieautoryzowanego połączenia, muszą zostać zapisane w odpowiednim dzienniku zdarzeń.
- Sieci teleinformatyczne ORLEN mogą być połączone z sieciami Stron Trzecich wyłącznie poprzez bezpieczny styk. Architektura bezpiecznego styku musi być ściśle uzależniona od jego przeznaczenia, ze szczególnym uwzględnieniem wymagań biznesowych oraz wymaganego poziomu ochrony.
- Komunikacja ze Stronami Trzecimi powinna być odpowiednio zabezpieczona poprzez zastosowanie kryptograficznych metod ochrony.

Separacja i segmentacja sieci OT

- Sieci Systemów OT muszą być odseparowane od innych sieci za pomocą odpowiednio skonfigurowanego urządzenia typu firewall. Zasady dostępu wyznacza (w tym m.in. konfigurację list ACL) Obszar Bezpieczeństwa (IT/OT).
- Wymiana Danych pomiędzy siecią danego Systemu OT, a innymi sieciami możliwa jest tylko poprzez dedykowaną strefę DMZ.
- Dozwolone jest używanie tylko tych portów, które są niezbędne dla zachowania prawidłowego funkcjonowania Systemu OT.
- W celu wzmocnienia izolacji Systemów OT, architektura sieci Systemów OT powinna opierać się na segmentacji sieci.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	33 / 40

5. Każdy segment sieci powinien być przypisany do funkcjonalnych warstw komponentów Systemów OT oraz metod komunikacji.
6. Cyberbezpieczeństwo przepływu danych i próby dostępu monitorowane są przez Obszar Bezpieczeństwa (IT/OT).

Usługi sieciowe

1. Zabronione jest używanie protokołów nieszyfrowanych m.in. http, FTP.
2. Komunikacja sieciowa Systemów OT z innymi sieciami powinna być inicjowana od strony Systemów OT.

VI. Monitorowanie Systemów OT

Monitorowanie zdarzeń

1. Wszystkie wdrażane Systemy OT powinny spełniać wymagania cyberbezpieczeństwa opisane w standardzie "Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS - OT" w szczególności zapewnić możliwość tworzenia i monitorowania dzienników zdarzeń dotyczących systemu operacyjnego w celu umożliwienia rejestracji działań Użytkowników na wszystkich komponentach w zakresie wymagań cyberbezpieczeństwa oraz wymagań prawnych.
2. Dziennik zdarzeń należy zabezpieczyć przed modyfikacją i nieuprawnionym dostępem.
3. Dzienniki zdarzeń powinny bazować na poprawnym mechanizmie synchronizacji czasu.
4. Dostęp do dzienników zdarzeń należy zapewnić w trybie „tylko do odczytu” Inżynierom OT, osobom z Obszaru Cyberbezpieczeństwa (IT/OT) oraz dedykowanym rozwiązaniom cyberbezpieczeństwa wskazanym przez Obszar Cyberbezpieczeństwa (IT/OT).

Monitorowanie komponentów i aplikacji

1. Monitorowanie wydajności, zajętości przestrzeni dyskowej i obciążenia poszczególnych komponentów Systemów OT powinno być prowadzone w trybie ciągłym z zapewnieniem odpowiedniej reakcji na ewentualne przyszłe problemy związane z dostępnością zasobów.
2. Monitorowanie aplikacji Systemów OT oraz infrastruktury teleinformatycznej pracującej wspólnie z tymi systemami, takiej jak urządzenia aktywne, serwery, systemy antywirusowe itp., należy prowadzić i rejestrować w trybie ciągłym.

VII. Zarządzanie incydentami

1. Incydenty bezpieczeństwa teleinformatycznego muszą być wykrywane, rejestrowane i monitorowane w sposób ciągły w celu ich identyfikowania i zapobiegania ich wystąpieniu w przyszłości.
2. Dobór działań i środków reagowania na przypadki naruszenia bezpieczeństwa zasobów informatycznych powinien być adekwatny do zagrożenia dla działalności operacyjnej ORLEN i potencjalnych strat.
3. Wszystkie incydenty w zakresie cyberbezpieczeństwa powinny być niezwłocznie zgłaszane do osób odpowiedzialnych za ich obsługę, zgodnie z obowiązującą procedurą.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	34 / 40

- Osoby odpowiedzialne za obsługę incydentów bezpieczeństwa teleinformatycznego, uprawnione są do działań zabezpieczających przed eskalacją / propagowaniem wykrytego zagrożenia oraz koordynowania działań, w tym działań Inżynierów OT.
- Wykryte przypadki naruszenia bezpieczeństwa Danych należy odpowiednio udokumentować i raportować.
- Przypadki naruszenia cyberbezpieczeństwa muszą być wyjaśniane, a ich sprawca może za nie odpowiadać zgodnie z obowiązującymi przepisami prawa oraz regulacjami wewnętrznymi ORLEN.
- Zdarzenia systemowe powinny być przechowywane, jako materiał dowodowy zaistniałych incydentów związanych z bezpieczeństwem teleinformatycznym.
- Przyczyny wystąpienia naruszeń bezpieczeństwa Danych muszą być analizowane, a mechanizmy bezpieczeństwa odpowiednio modyfikowane w celu zminimalizowania ryzyka ponownego wystąpienia przypadków naruszenia bezpieczeństwa Danych.
- Dokumentacja incydentów bezpieczeństwa powinna zawierać opis incydentu wraz z przypisaną kategorią i priorytetem, czas zgłoszenia i rozwiązania incydentu, działania podejmowane po otrzymaniu zgłoszenia i ich właścicieli.

VIII. Zarządzanie zmianą

- Każda zmiana w Systemie OT musi być odpowiednio zaplanowana, uzgodniona z zainteresowanymi stronami, udokumentowana, zweryfikowana pod kątem bezpieczeństwa i musi być realizowana w sposób kontrolowany i przy zachowaniu formalnych zasad i procedur.
- Na przeprowadzenie zmiany w Systemach OT musi wyrazić zgodę jego Właściciel Biznesowy OT.
- Szczegółowe wytyczne dotyczące przeprowadzania zmian w Systemach OT zostały zawarte w odrębnym zarządzeniu.

Zarządzanie aktualizacjami

- Każdy komponent Systemu OT powinien być objęty planem zarządzania aktualizacjami, definiującym harmonogram sprawdzania dostępności aktualizacji i ich instalacji.
- Aktualizacja nie powinna obniżać poziomu bezpieczeństwa Systemu OT ani bezpieczeństwa żadnego innego elementu infrastruktury teleinformatycznej ORLEN.
- Instalowanie aktualizacji, których wpływ na działanie Systemu OT nie został zweryfikowany jest zabronione.
- Za wgrywanie aktualizacji oraz zarządzanie aktualizacjami Systemu OT odpowiedzialny jest Inżynier OT.

Zarządzanie konfiguracją

- Za zarządzanie konfiguracją Systemu OT odpowiedzialny jest Inżynier OT

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	35 / 40

- Systemy OT powinny być skonfigurowane w taki sposób, aby umożliwić korzystającym z nich Użytkownikom OT wykonywanie obowiązków służbowych.
- Funkcjonalności i serwisy, które nie są wykorzystywane, powinny być wyłączone lub zablokowane.
- Dostęp do plików konfiguracyjnych powinien być udzielony Użytkownikom OT jedynie w zakresie niezbędnym do wykonywania przez nich obowiązków służbowych.
- Nieautoryzowana zmiana konfiguracji aplikacji jest zabroniona.
- Konfigurację Systemów OT należy poddawać okresowym jak również niezapowiedzianym przeglądom.

IX. Bezpieczeństwo fizyczne i środowiskowe

Bezpieczeństwo fizyczne i środowiskowe

- W celu ochrony Systemów OT przed kradzieżą lub zniszczeniem należy stosować odpowiednie środki ochrony, uwzględniające obowiązujące wymagania prawne, regulacje wewnętrzne oraz normy.
- Pomieszczenia techniczne muszą spełniać wymogi prawa w zakresie ochrony przeciwpożarowej, norm branżowych oraz bezpieczeństwa i higieny pracy.
- Zasoby Systemów OT, powinny być rozmieszczane w strefach bezpieczeństwa zabezpieczonych przed dostępem osób niepowołanych.
- Umieszczenie oraz stosowane środki ochrony muszą uwzględniać obowiązujące wymagania prawne, potrzeby biznesowe oraz wyniki przeprowadzonej weryfikacji bezpieczeństwa w tym zakresie.
- Lokalizację i umiejscowienie komponentów Systemów OT należy dobierać z uwzględnieniem ryzyka mogącego powodować zagrożenie dla bezpieczeństwa Systemów OT, bezpieczeństwa pracy komponentów Systemów OT i przechowywania nośników informacji. W szczególności należy rozważyć aspekty dotyczące:
 - Zasilania energią elektryczną;
 - Klimatyzacji oraz wentylacji;
 - Wykrywania oraz ochrony przed pożarem i zalaniem;
 - Fizycznej kontroli dostępu.
- Pomieszczenia techniczne należy wyposażyć w odpowiednie środki ochrony fizycznej i organizacyjnej, chroniące przed zdarzeniami mogącymi spowodować kradzież, uszkodzenia, nieuprawniony dostęp, zakłócenie pracy Systemów OT.

Zasoby Systemów OT muszą być zasilane napięciem zgodnym z wymogami postawionymi przez producenta danego sprzętu

- Powinny być chronione przed awariami sieci elektroenergetycznych.
- Należy stosować środki organizacyjne i techniczne w celu ochrony Systemów OT, Nośników Elektronicznych i urządzeń elektronicznych, danych wejściowych i wyjściowych oraz

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	36 / 40

dokumentacji systemowej przed nieautoryzowanym lub nieuprawnionym ujawnieniem, modyfikacją, usunięciem i zniszczeniem.

Kontrola dostępu do systemów automatyki przemysłowej

1. Kontrola dostępu do Systemów OT jest funkcją bezpieczeństwa, która pozwala na dostęp wyłącznie dla osób uprawnionych.
2. Kontrola dostępu do Systemów OT powinna być prowadzona zgodnie z potrzebami biznesowymi oraz wymaganiami bezpieczeństwa. W szczególności kontrola dostępu powinna wynikać z następujących aspektów:
 - 2.1. Rodzaju przetwarzanych Danych.
 - 2.2. Zgodności z wymaganiami prawa i umowami.
 - 2.3. Zasady wiedzy koniecznej.
3. Zasoby Systemów OT powinny posiadać mechanizmy ochrony przed nieautoryzowanym dostępem.
4. Zasoby Systemów OT powinny posiadać mechanizmy rejestrowania zdarzeń dotyczących dostępu i prób dostępu, które powinny być przechowywane zgodnie z ustalonymi okresami przechowywania tego typu zdarzeń.
5. Zasoby Systemów OT, jeżeli technologicznie jest to możliwe, powinny posiadać mechanizmy zapewniające ograniczanie liczby prób wprowadzania hasła i po przekroczeniu limitu (maksymalnie 10 prób), logowanie na dany identyfikator i hasło Użytkownika OT powinno być blokowane na stałe lub czasowo. Jest to szczególnie istotne w przypadku haseł z założenia bardzo krótkich (np. PIN). W takim przypadku należy stosować ograniczenie do 3 prób.
6. Zasoby Systemów OT, jeśli to technicznie realizowalne, powinny umożliwiać wyświetlanie daty i czasu ostatniego udanego i nieudanego logowania.
7. Niewykorzystywane konta Użytkowników OT należy zablokować.

x.Zarządzanie ciągłością działania

1. W celu zapewnienia odpowiedniej oraz oczekiwanej dostępności Systemów OT powinno stosować się wszelkie dostępne i adekwatne środki. Środki wykorzystywane w celu utrzymania ciągłości działania Systemów OT muszą być adekwatne do akceptowalnego poziomu ryzyka.
2. Dla zapewnienia właściwego reagowania i przebiegu prac dla Systemów OT w przypadku wstąpienia poważnej awarii lub katastrofy należy opracować i wdrożyć dokumentację zarządzania ciągłością działania.
3. Na cały proces zarządzania ciągłością działania w Obszarze Informatyki składają się zasoby sprzętowe, programowe oraz szczegółowe procedury operacyjne związane z funkcjonowaniem planu zarządzania ciągłością działania. Głównym zadaniem jest zapewnienie realizacji działalności biznesowej Spółki dla uzgodnionych Systemów OT w przypadku wystąpienia poważnej awarii lub katastrofy danego Systemu OT.
4. Głównym celem dokumentacji zarządzania ciągłością działania jest wyznaczenie zasad organizacji pracy, zmierzające do utrzymania ciągłości działania uzgodnionych Systemów OT, minimalizacja wpływu poważnej awarii lub katastrofy oraz możliwie sprawne przywrócenie poprawnego funkcjonowania danego Systemu OT.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	37 / 40

- Aktualizacja dokumentacji zarządzania ciągłością działania powinna być prowadzona regularnie i adekwatnie do zmian technicznych i operacyjnych mających wpływ na funkcjonowanie Systemów OT.
- Dokumentacja zarządzania ciągłością działania oraz poszczególne polityki, instrukcje i procedury odtworzenia danego Systemu OT powinny być adekwatne do potrzeb, możliwości i warunków panujących w otoczeniu ORLEN oraz powinny zapewniać możliwość przywrócenia sprawności Systemu OT po całkowitym lub częściowym uszkodzeniu danego Systemu OT, spowodowanym naturalnym kataklizmem, takim jak powódź czy pożar lub innymi czynnikami, tj. awariami sprzętu lub działaniami celowymi.
- Dla Systemów OT niezbędnych do zapewnienia ciągłości działalności procesów biznesowych ORLEN powinny istnieć mechanizmy pozwalające zidentyfikować zdarzenia mogące przerwać lub zakłócić poprawne działanie Systemów OT.
- Umowy z dostawcami Systemów OT muszą określać m.in. czas reakcji zgodnie z planem utrzymania oraz odtworzenia danego Systemu OT.

xi. Weryfikacja stanu cyberbezpieczeństwa

Zmiany w Systemach OT wymagają efektywnego monitorowania oraz wewnętrznych i zewnętrznych audytów i przeglądów bezpieczeństwa w celu wykrywania potencjalnych nowych zagrożeń i zmiany poziomów ryzyka.

Przeglądy bezpieczeństwa Systemów OT są podstawowym procesem mającym na celu ocenę ogólnego stanu bezpieczeństwa zasobów oraz weryfikację właściwego działania istniejących zabezpieczeń. Przeglądy bezpieczeństwa pozwalają uzyskać obiektywną informację na temat obecnego środowiska teleinformatycznego i jego zabezpieczeń w odniesieniu do PBTi.

Niniejszy rozdział zawiera następujące wytyczne odnośnie procesu przeglądu bezpieczeństwa Systemów OT w ORLEN:

- Systemy OT powinny być okresowo poddawane niezależnym i obiektywnym przeglądom bezpieczeństwa w celu określenia spełnienia wymaganego poziomu zabezpieczeń pozwalającego na ograniczenie ryzyka do poziomu akceptowalnego.
- Za przeprowadzanie przeglądów bezpieczeństwa Systemów OT odpowiedzialny jest Obszar Cyberbezpieczeństwa (IT/OT).
- Wszelkie działania związane z przeglądem, audytem lub kontrolą bezpieczeństwa Systemów OT należy realizować za zgodą Obszaru Cyberbezpieczeństwa (IT/OT) lub przełożonych.
- W przypadku naruszenia bezpieczeństwa lub wykrycia podatności dla danego Systemu OT powinien zostać przeprowadzony przegląd bezpieczeństwa.
- Przed przystąpieniem do przeglądu bezpieczeństwa Systemów OT należy zdefiniować zakres, budżet, czas przeprowadzenia przeglądu oraz uzyskać zgodę Obszaru Cyberbezpieczeństwa (IT/OT).
- Podczas przeglądu bezpieczeństwa powinny zostać zidentyfikowane słabości/podatności dla Systemów OT oraz przedstawione rekomendacje wraz z priorytetem ich wdrożenia.
- Każdorazowo należy przedstawić do weryfikacji i akceptacji Obszaru Cyberbezpieczeństwa (IT/OT) zidentyfikowane słabości/podatności oraz rekomendacje z priorytetami z obszaru, w którym zidentyfikowano podatności i zagrożenia.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	38 / 40

8. Po zakończeniu wdrożenia poszczególnych rekomendacji lub ich zaniechania osoba z Obszaru Cyberbezpieczeństwa (IT/OT) powinna zweryfikować czy rekomendacja została wdrożona prawidłowo lub czy zaniechanie wdrożenia rekomendacji zostało prawidłowo uzasadnione.
9. Narzędzia informatyczne służące do przeprowadzania przeglądów bezpieczeństwa teleinformatycznego powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem, a ich użycie odpowiednio kontrolowane.

INŻYNIEROWIE FIRM ZEWNĘTRZNYCH (OT) W SYSTEMACH OT

I. Zasady zarządzania dostępem

1. Inżynierowie Firm Zewnętrznych (OT) powinni zapobiegać nieautoryzowanemu i nieuprawnionemu dostępowi, naruszeniu bezpieczeństwa, kradzieży lub uszkodzeniu Systemów OT.
2. Wszelkie czynności mogące umożliwić nieuprawniony dostęp do Systemów OT są zabronione.
3. Zakres uprawnień do Systemów OT każdego z Inżynierów Firm Zewnętrznych (OT) powinien być ograniczony do minimalnego, niezbędnego do wykonywania ustalonych z Inżynierem OT lub Obszarem Cyberbezpieczeństwa (IT/OT) zadań.
4. Nadanie Inżynierowi Firm Zewnętrznych (OT) uprawnień do poszczególnych komponentów Systemów OT musi odbywać się formalnie, zgodnie z obowiązującymi zasadami zarządzania uprawnieniami.
5. Inżynier Firm Zewnętrznych (OT) może używać jedynie precyzyjnie określonych kont w celu logowania do Systemów OT.
6. Inżynier Firm Zewnętrznych (OT) może się logować jedynie do zasobów Systemu OT, które są niezbędne do wykonywania ustalonych z Inżynierem OT lub Obszarem Cyberbezpieczeństwa (IT/OT) zadań.
7. Inżynier Firm Zewnętrznych (OT) może przebywać w pomieszczeniach, w których znajdują się komponenty Systemu OT jedynie pod nadzorem pracownika Spółki.

II. Ochrona przed szkodliwym oprogramowaniem

1. Ochrona przed szkodliwym oprogramowaniem (przestępcze lub złośliwe działanie w stosunku do Systemów OT) powinna być ukierunkowana na niezwłoczne wykrywanie oraz usuwanie lub blokowanie szkodliwego oprogramowania.
2. W celu uniknięcia destrukcyjnych oraz kosztownych implikacji, jakie mogą być wywołane działaniem szkodliwego oprogramowania, ochrona antywirusowa musi być zgodna i aktualna.
3. Inżynier Firm Zewnętrznych (OT) na wykorzystywanych stacjach komputerowych oraz serwerach Systemu OT powinien mieć aktywne oprogramowanie antymalware (dotyczy tylko określonych komponentów Systemów OT).
4. Inżynier Firm Zewnętrznych (OT) bez zgody Obszaru Cyberbezpieczeństwa (IT/OT) nie może dezaktywować oprogramowania antywirusowego ani antymalware.

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	39 / 40

III. Instalowanie/odinstalowywanie oraz uruchamianie/wyłączanie oprogramowania

1. Inżynierowie Firm Zewnętrznych (OT) bez zgody Inżyniera OT nie są uprawnieni do samodzielnego instalowania oprogramowania na jakichkolwiek urządzeniach Spółki, takich jak m.in. stacje systemów automatyki przemysłowej.
2. Inżynierowie Firm Zewnętrznych (OT) bez zgody Inżyniera OT lub Obszaru Cyberbezpieczeństwa (IT/OT) nie mogą instalować ani odinstalowywać żadnego oprogramowania w Systemie OT.
3. W przypadku zaistnienia potrzeby, instalacja oprogramowania jest prowadzona przez Inżyniera OT i zgodnie z obowiązującymi zasadami w tym zakresie.
4. Inżynierowie Firm Zewnętrznych (OT) nie mogą uruchamiać w Systemie OT innych niż zainstalowanych systemów operacyjnych.

IV. Sieć teleinformatyczne

1. Dostęp do sieci Internet z zasobów Systemów OT lub dowolnego elementu podłączonego do sieci Systemów OT jest zabroniony.
2. Bezpośredni dostęp do Systemów OT z sieci Internet jest zabroniony.
3. Dostęp do Systemu OT spoza sieci Systemów OT (z wyłączeniem sieci Internet) powinien być możliwy wyłącznie dla autoryzowanych usług i Inżynierów Firm Zewnętrznych (OT) z wykorzystaniem autoryzowanych protokołów i środków uwierzytelniających. Autoryzacji może dokonać jedynie Obszar Cyberbezpieczeństwa (IT/OT).
4. Inżynierowie Firm Zewnętrznych (OT) nie mogą podłączać komponentów Systemów OT do sieci teleinformatycznych.
5. Bez zgody Inżyniera OT lub Obszaru Cyberbezpieczeństwa (IT/OT), Inżynierowie Firm Zewnętrznych (OT) nie mogą podłączać żadnych zasobów teleinformatycznych do sieci teleinformatycznych Spółki, w szczególności do Systemów OT.

V. Poczta elektroniczna

1. Korzystanie przez Inżynierów Firm Zewnętrznych (OT) z poczty elektronicznej poprzez zasoby Systemów OT lub dowolne elementy podłączone do sieci Systemów OT jest zabronione.

VI. Nośniki Elektroniczne

1. Inżynierowie Firm Zewnętrznych (OT) nie mogą podłączać do Systemu OT nośników zewnętrznych (np. pamięci masowych USB, płyt CD/DVD)

VII. Zarządzanie incydentami

1. Inżynier Firm Zewnętrznych (OT) zobowiązany jest zgłosić do osoby nadzorującej pracę każdy zaistniały incydent natychmiast po jego wystąpieniu:
 - 1.1. za pośrednictwem poczty e-mail wysyłając informację na adresy: soc@orlen.pl; cert@orlen.pl.
 - 1.2. Telefonicznie dzwoniąc na numer +48 24 256 90 90 lub +48 887 520 250;

	Standard Cyberbezpieczeństwa OT Zasady Bezpieczeństwa Teleinformatycznego OT	Wersja:	4.0
		Data:	2025-01-21
		Strona:	40 / 40

- 1.3. Zgłaszając incydent Cyberbezpieczeństwa poprzez system HelpDesk (Zgłoszenie w klasyfikacji: Informatyka / Cyberbezpieczeństwo / Zgłoś incydent Cyberbezpieczeństwa / Zgłoś incydent Cyberbezpieczeństwa).

VIII. Zarządzanie zmianą

1. Zmiany w zakresie konfiguracji komponentów oraz funkcjonalności Systemów OT mogą być dokonywane jedynie przez Inżyniera OT lub osoby przez niego wskazane.
2. Zmiany w zakresie konfiguracji cyberbezpieczeństwa w Systemach OT muszą być dokonywane po akceptacji Obszaru Cyberbezpieczeństwa (IT/OT).

Postanowienia końcowe

Właścicielem niniejszego standardu jest Obszar Cyberbezpieczeństwa OT ORLEN S.A. Jakiegolwiek 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 Obszaru Cyberbezpieczeństwa OT ORLEN S.A.