
	<b>Standard Cyberbezpieczeństwa OT</b> <hr/> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	1 z 19



## Standard Cyberbezpieczeństwa OT


---

Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT  
**Polityka Bezpieczeństwa Teleinformatycznego OT**  
**dla stron trzecich**

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	2 z 19

## Spis treści


DEFINICJE.....	3
PREAMBUŁA .....	7
OGÓLNE ZASADY CYBERBEZPIECZEŃSTWA .....	9
I.    Podstawowe zasady zarządzania dostępem .....	9
II.   Poufność i bezpieczeństwo Zasobów Teleinformatycznych IT oraz Systemów OT.....	9
V.    Poufność i dostępność Danych.....	11
VI.   Poziom Bezpieczeństwa Teleinformatycznego / Cyberbezpieczeństwa i jego weryfikacja ..	12
VII.  Zasada wiedzy koniecznej .....	12
VIII. Wykorzystywanie Zasobów Teleinformatycznych IT oraz Systemów OT.....	12
IX.   Bezpieczeństwo formalno-prawne.....	13
X.    Polityka „czystego biurka” i Polityka „czystego ekranu” .....	13
XI.   Ochrona przed inżynierią społeczną (socjotechniką) .....	14
XII.  Niedozwolone czynności .....	14
<b>CYBERBEZPIECZEŃSTWO OT - SYSTEMY OT .....</b>	<b>18</b>
INŻYNIEROWIE FIRM ZEWNĘTRZNYCH (OT) W SYSTEMACH OT .....	18
I.    Zasady zarządzania dostępem.....	18
II.   Ochrona przed szkodliwym oprogramowaniem .....	18
III.  Instalowanie/odinstalowywanie oraz uruchamianie/wyłączanie oprogramowania .....	18
IV.   Sieć teleinformatyczne .....	19
V.    Poczta elektroniczna.....	19
VI.   Nośniki Elektroniczne .....	19
VII.  Zarządzanie incydentami.....	19
VIII. Zarządzanie zmianą .....	19

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	3 z 19


## DEFINICJE

### 1. 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.

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	4 z 19

- 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** – PKN ORLEN S.A. oraz spółki, w których PKN 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 PKN ORLEN w Obszarze Informatyki komórka organizacyjna odpowiedzialna za Cyberbezpieczeństwo (IT oraz OT).
- 1.17. **Obszar Informatyki – Komórka Organizacyjna PKN ORLEN, dalej Obszar IT.**
- 1.18. **OT Cybersecurity** – powołany na potrzeby całego Koncernu, centralny zespół cyberbezpieczeństwa OT w strukturze organizacyjnej Obszaru Informatyki PKN 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.


	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	5 z 19

- 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

	<b>Standard Cyberbezpieczeństwa OT</b> <hr/> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	6 z 19

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.

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	7 z 19

## PREAMBUŁA

### Wstęp


1. Niniejszy dokument został przygotowany na bazie obowiązującej Polityki Bezpieczeństwa Teleinformatycznego w Koncernie i określa zasady, do których powinni stosować się pracownicy stron trzecich i firm zewnętrznych.
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.

### 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.

### Zakres stosowania

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


	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	8 z 19

- 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.

### *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 PKN ORLEN zasad Bezpieczeństwa Teleinformatycznego / Cyberbezpieczeństwa, w tym zdefiniowanych przez niniejszą PBTi.
  - 2.2. Zapewnienie wykonywania obowiązków wynikających z ustaleń z PKN ORLEN w sposób zapobiegający utracie Poufności, Integralności i Dostępności Zasobów Teleinformatycznych IT oraz Systemów OT.
  - 2.3. Zapobieganie nieuprawnionemu dostępowi do udostępnionych przez PKN 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 PKN ORLEN protokołów, usług i uprawnień.
  - 2.6. Korzystanie z udostępnionych przez PKN 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.
  - 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 PKN ORLEN, w tym zakresie (tu: zgłoszenie do HelpDesk PKN 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.



	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	9 z 19

## 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:
  - 2.1. Długość co najmniej 10 znaków dla standardowego konta Użytkownika.
  - 2.2. Długość co najmniej 14 znaków dla konta uprzywilejowanego.

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	10 z 19

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


- Hasel nie należy zapisywać i pozostawiać w miejscu, w którym mogłyby zostać ujawnione.
- Hasel nie należy przechowywać w plikach, systemach, aplikacjach, bazach danych, skryptach i plikach konfiguracyjnych bez zapewnienia im poufności środkami technicznymi lub co najmniej organizacyjnymi.

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	11 z 19

- Hasła nie powinny być wpisywane w obecności innych osób, jeśli mogą one zauważyć treść wpisywanego hasła.
- 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.
- 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.
- Hasła do kont uprzywilejowanych należy objąć szczególną ochroną.
- Hasła należy przechowywać w sposób bezpieczny, zapewniający im poufność, dostępność oraz rozliczalność ich wykorzystania.
- Hasła należy utrzymywać w tajemnicy również po upływie ich ważności.
- W przypadku podejrzenia ujawnienia hasła, należy niezwłocznie skontaktować się z HelpDesk i przekazać stosowną informację.

## **v. Poufność i dostępność Danych**

- Nośniki Elektroniczne, muszą być zabezpieczane zgodnie z przyjętymi w Spółce zasadami.
- Dostęp do Nośników Elektronicznych powinni posiadać tylko uprawnieni Użytkownicy lub osoby posiadające potwierdzenie z Obszaru Bezpieczeństwa IT/OT.
- 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.
- 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.
- W przypadku komputerów przenośnych oraz komputerów stacjonarnych w uzasadnionych przypadkach powinny być stosowane filtry prywatyzujące.
- Wszelkie Dane przetwarzane w związku z obowiązkami służbowymi powinny być przechowywane na dedykowanych do tego celu zasobach (np. współdzielone lub indywidualne zasoby sieciowe).
- Odpowiedzialność za właściwą Dostępność oraz Poufność Danych spoczywa na Użytkowniku przetwarzającym te Dane, w zakresie dotyczącym danego Użytkownika.
- Zabronione jest wykorzystywanie prywatnych skrzynek pocztowych znajdujących się poza domeną pocztową PKN ORLEN do przetwarzania Danych związanych z wykonywanymi obowiązkami służbowymi.
- Do przetwarzania Danych związanych z wykonywanymi obowiązkami służbowymi wykorzystywane może być jedynie konto służbowej korporacyjnej poczty elektronicznej Koncernu.

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	12 z 19

## VI. Poziom Bezpieczeństwa Teleinformatycznego / Cyberbezpieczeństwa i jego weryfikacja


1. Niedozwolone jest wykorzystywanie logicznych lub sprzętowych luk w Zasobach Teleinformatycznych IT oraz Zasobach Teleinformatycznych OT.
2. 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.
3. Użytkownicy eksploatujący Zasoby Teleinformatyczne IT lub Zasoby Teleinformatyczne OT są odpowiedzialni za zabezpieczenie wykorzystywanych komponentów przed nieuprawnionym dostępem, uszkodzeniem i utratą.
4. Użytkownicy są zobowiązani do współpracy i terminowości przy prowadzonych pracach związanych bezpośrednio z Bezpieczeństwem Teleinformatycznym IT lub Zasoby Teleinformatyczne OT dotyczących np. wgrywania uaktualnień (systemu operacyjnego, aplikacji, systemu antywirusowego).
5. Wszelkie incydenty Bezpieczeństwa Teleinformatycznego / Cyberbezpieczeństwa należy niezwłocznie zgłaszać do HelpDesk.

## VII. Zasada wiedzy koniecznej

1. 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

1. 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.
2. 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.
3. 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.
4. Wszelkie materiały (np. dokumenty) wytworzone przy użyciu Zasobów Teleinformatycznych IT oraz Systemów OT Spółki stanowią własność Spółki, chyba że odrębne umowy stanowią inaczej.

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	13 z 19


- Wykorzystywanie Zasobów Teleinformatycznych IT oraz Zasobów Teleinformatycznych, w tym poszczególnych usług informatycznych może być rejestrowane i monitorowane przez systemy i urządzenia Spółki.
- Jedynie autoryzowane oraz uprawnione osoby mogą monitorować dzienniki zdarzeń oraz Dane z Zasobów Teleinformatycznych IT oraz Systemów OT.
- 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.
- 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

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

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

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

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	14 z 19

## **XI. Ochrona przed inżynierią społeczną (socjotechniką)**


- 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.
- Techniki wykorzystywane przez intruza przy inżynierii społecznej polegają m.in. na:
  - Powoływaniu się na pilną sprawę o wysokim znaczeniu dla PKN ORLEN lub innego podmiotu.
  - Oferowaniu pomocy technicznej np. w przypadku zagrożenia wirusem komputerowym, awarią lub weryfikacją uprawnień.
  - Próbach wymuszenia działań na Użytkowniku i powoływaniu się przy tym na osoby z wyższego szczebla, np. na przełożonego.
  - Podszywaniu się pod inną osobę.
  - Wzbudzeniu zaufania oraz prawieniu komplementów.
  - Uzyskiwaniu informacji, które mogą być informacjami podlegającymi ochronie na mocy przepisów prawa np. hasła, informacje dotyczące kontrahentów lub współpracowników, informacje dotyczące stosowanych zabezpieczeń, itp.
  - Powoływaniu się na znajomość pracowników PKN ORLEN.
- Zazwyczaj techniki są wykorzystywane przez osobę trzecią za pomocą dostępnych środków komunikacji, takich jak telefon, poczta elektroniczna, Internet, rzadziej osobiście.
- 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.
- 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.

### **1. Systemy i sieci teleinformatyczne:**

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	15 z 19

- 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 PKN 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.
- 1.13. Wykorzystywanie nieautoryzowanych przez Obszar Bezpieczeństwa IT/OT mechanizmów służących do ustanowienia zdalnego dostępu do Zasobów teleinformatycznych PKN ORLEN.
- 1.14. Udostępnianie usługi zdalnego dostępu do Zasobów Teleinformatycznych IT lub Systemów OT osobom nieuprawnionym.



	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	16 z 19

- 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 PKN ORLEN bez akceptacji Dyrektora Wykonawczego ds. Informatyki, w tzw. „Chmurze” (ang. Cloud Computing), to jest w systemach typu „eroom”, „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 PKN 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 PKN ORLEN do przetwarzania Danych związanych z wykonywanymi obowiązkami służbowymi.
- 4.2. Podszywanie 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



	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	17 z 19

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 PKN ORLEN i niezgodnionych z właściwą komórką organizacyjną PKN 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 PKN 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.

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	18 z 19

## CYBERBEZPIECZEŃSTWO OT - SYSTEMY OT

### 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

- 1.1. 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.
- 1.2. W celu uniknięcia destrukcyjnych oraz kosztownych implikacji, jakie mogą być wywołane działaniem szkodliwego oprogramowania, ochrona antywirusowa musi być zgodna i aktualna.
- 1.3. Inżynier Firm Zewnętrznych (OT) na wykorzystywanych stacjach komputerowych oraz serwerach Systemu OT powinien mieć aktywne oprogramowanie antymalware (dotyczy tylko określonych komponentów Systemów OT).
- 1.4. Inżynier Firm Zewnętrznych (OT) bez zgody Obszaru Cyberbezpieczeństwa (IT/OT) nie może dezaktywować oprogramowania antywirusowego ani antymalware.

#### 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.

	<b>Standard Cyberbezpieczeństwa OT</b> Załącznik nr 4 do Standardu Cyberbezpieczeństwa OT - <b>Polityka Bezpieczeństwa</b> Teleinformatycznego OT dla stron trzecich	Wersja:	I
		Data wydania:	2023-04-13
		Strona:	19 z 19

- Inżynierowie Firm Zewnętrznych (OT) bez zgody Inżyniera OT lub Obszaru Cyberbezpieczeństwa (IT/OT) nie mogą instalować ani odinstalowywać żadnego oprogramowania w Systemie OT.
- W przypadku zaistnienia potrzeby, instalacja oprogramowania jest prowadzona przez Inżyniera OT i zgodnie z obowiązującymi zasadami w tym zakresie.
- Inżynierowie Firm Zewnętrznych (OT) nie mogą uruchamiać w Systemie OT innych niż zainstalowanych systemów operacyjnych.

#### IV.Sieć teleinformatyczne

- Dostęp do sieci Internet z zasobów Systemów OT lub dowolnego elementu podłączonego do sieci Systemów OT jest zabroniony.
- Bezpośredni dostęp do Systemów OT z sieci Internet jest zabroniony.
- 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).
- Inżynierowie Firm Zewnętrznych (OT) nie mogą podłączać komponentów Systemów OT do sieci teleinformatycznych.
- 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

- 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

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

#### VII.Zarządzanie incydentami

- Inżynier Firm Zewnętrznych (OT) zobowiązany jest zgłosić do osoby nadzorującej pracę każdy zaistniały incydent natychmiast po jego wystąpieniu.

#### VIII.Zarządzanie zmianą

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