

PROCEDURA OGÓLNA ZARZĄDZANIA ZDALNYM DOSTĘPEM DO SIECI KORPORACYJNEJ (VPN)

PROG 00041 / A

Sygn.: PGE/CENT/DSIT/4.07

Data zatwierdzenia: 2015/06/10
Obowiązuje od: 2015/06/10

I CEL I ZAKRES

- 1.1 Celem Procedury Ogólnej zarządzania zdalnym dostępem do Sieci Korporacyjnej (VPN) jest ustanowienie zasad nadawania zdalnego dostępu do Sieci Korporacyjnej Grupy PGE z wykorzystaniem VPN, obsługiwanego przez CUW ICT.
- 1.2 Procedura Ogólna obejmuje swoim zakresem zarządzanie dostępem do Sieci Korporacyjnej z wykorzystaniem mechanizmów zdalnego dostępu VPN dotyczy korporacyjnej domeny Grupy PGE, administrowanych przez CUW ICT.
- 1.3 Stosownie do zapisów Kodeksu Grupy PGE, Dokumenty Systemu Zarządzania Grupy PGE, są wydawane w celu osiągnięcia takich wartości jak:
 - a. spójność działania Spółek,
 - b. przejrzystość działania Spółek i Grupy PGE,
 - c. zwiększenie efektywności i skuteczności kontroli procesów biznesowych, organizacyjnych i prawnych w Grupie PGE,
- 1.4 ograniczenia ryzyk biznesowych Podstawę uchwalenia Procedury stanowi Rozdział 5 Kodeksu Grupy PGE oraz postanowienia statutów (umów) Spółek.
- 1.5 Postanowienia DSZ należy wyklądać w duchu Kodeksu Grupy PGE.

II ODPOWIEDZIALNOŚĆ

- 2.1 Za stosowanie wymagań niniejszej Procedury odpowiedzialne są Spółki a w szczególności:
 - a. wszyscy Pracownicy Spółki, Członkowie Organów Spółki i Osoby Trzecie realizujące określone zadania na rzecz Spółki,
 - b. Dyrektor Departamentu Strategii IT Grupy Kapitałowej PGE w zakresie aktualizacji Procedury,
- 2.1.2 Do Spółek z Grupy PGE Procedura ma bezpośrednie zastosowanie.
- 2.1.3 Do Spółek innych niż Spółki z Grupy PGE, stosowanie postanowień Procedury odbywa się odpowiednio za pomocą rozwiązań stosownych do danego przypadku za pośrednictwem:
 - a. Spółek z Grupy PGE - dla spółek zależnych od Spółek z Grupy PGE, lub
 - b. jednostki w Grupie PGE, która ma w swoich podstawowych zadaniach zarządzanie korporacyjne w Grupie PGE – dla pozostałych Spółek.
- 2.2 Wszelkie odstępstwa od niniejszej Procedury muszą być zaakceptowane przez Dyrektora Departamentu Strategii IT w PGE S.A.

III DOKUMENTY POWIĄZANE

- 3.1 PROG 00039 Procedura Ogólna bezpieczeństwa teleinformatycznego
- 3.2 PROG 00040 Procedura Ogólna zarządzania dostępem do podstawowych zasobów informatycznych Grupy PGE
- 3.3 Kodeks Grupy PGE

IV ZAŁĄCZNIKI

- 4.1 [Załącznik 1](#) Oświadczenie dotyczące pracy zdalnej (VPN)
- 4.2 [Załącznik 2](#) Wniosek o nadanie / modyfikację uprawnień do zdalnego dostępu VPN
- 4.3 [Załącznik 3](#) Wniosek o odebranie zdalnego dostępu VPN
- 4.4 [Załącznik 4](#) Wniosek o utworzenie / modyfikację Profilu Zdalnego Dostępu VPN
- 4.5 [Załącznik 5](#) Wniosek o usunięcie Profilu Zdalnego Dostępu VPN

V SKRÓTY I DEFINICJE

CUW ICT:

Skróty użyte na potrzeby niniejszego dokumentu:

- CUW ICT** – Centrum Usług Wspólnych ICT - podmioty, których celem jest świadczenie usług ICT na rzecz pozostałych spółek Grupy PGE w oparciu o model optymalizujący efektywność ICT w Grupie PGE. Rolę CUW ICT pełnią trzy spółki:
- a. PGE Systemy w zakresie usług informatycznych,
 - b. Exatel w zakresie usług telekomunikacyjnych,
 - c. Energo-Tel w zakresie usług eksploatacji, serwisu sieci i infrastruktury telekomunikacyjnej.
- Exatel nie jest CUW ICT w rozumieniu ustawy Prawo Zamówień Publicznych. W odróżnieniu od PGE Systemy oraz Energo-Tel, Exatel większość swoich usług świadczy poza Grupę PGE
- ICT** – teleinformatyka - dziedzina łącząca informatykę, telekomunikację oraz narzędzia i inne technologie związane z Przetwarzaniem Informacji. Nie obejmuje rozwiązań związanych z teleinformatyką przemysłową i automatyką. W sytuacji wątpliwej w zakresie granicy ICT oraz teleinformatyki przemysłowej i automatyzacji, bądź też konieczności wyłączenia fragmentu obszaru z definicji Usługi ICT stosowne decyzje będzie podejmował Komitet ICT
- System OW** - System teleinformatyczny do obsługi Wniosków
- VPN** – (ang. Virtual Private Network), wirtualna sieć prywatna, tunel między dwoma punktami sieci (np. laptopem, a siecią wewnętrzną Banku), który umożliwia bezpieczną transmisję danych np. poprzez sieć publiczną Internet
- ZZL** - Zarządzanie Zasobami Ludzkimi

Definicje pojęć użyte na potrzeby niniejszego dokumentu:

- 5.1 **Administrator Techniczny (Administrator)** – Pracownik CUW ICT lub Osoba Trzecia posiadająca odpowiedni poziom uprawnień i odpowiedzialności za System Teleinformatyczny lub element infrastruktury teleinformatycznej. Osoba ta zarządza i sprawuje nadzór nad Systemem Teleinformatycznym lub innym elementem infrastruktury teleinformatycznej od strony technicznej.
- 5.2 **Jednostka organizacyjna** - organizacja powołana do wykonywania określonych części zadań w Spółce, mająca ustalone miejsce w jej strukturze organizacyjnej. Jednostką organizacyjną może być oddział.
- 5.3 **Kierownik Komórki organizacyjnej** - osoba kierująca Komórka organizacyjną w rozumieniu Regulaminu organizacyjnego Spółki.
- 5.4 **Komórka organizacyjna / Komórka** - jedno - lub wieloosobowe ciało powołane do wykonywania określonych części zadań w jednostce organizacyjnej, mające ustalone miejsce w jej strukturze organizacyjnej. Komórką może być: departament, biuro, zespół, wydział, dział, sekcja lub inna komórka wewnętrzna w Spółce lub oddziale Spółki
- 5.5 **Nadzorca Dostępu do Usługi (Nadzorca Dostępu)** - osoba w strukturze organizacyjnej Spółki sprawująca nadzór nad dostępem do Usługi dla określonej grupy Użytkowników.
- 5.6 **Opiekun Osoby Trzeciej** – Kierownik Komórki organizacyjnej, w ramach której Osoba Trzecia realizuje swoje zadania lub Pracownik tej Komórki organizacyjnej posiadający pisemne upoważnienie wydane przez powyższego Kierownika.
- 5.7 **Organy Spółki** – Organy Spółki w rozumieniu Regulaminu Organizacyjnego Spółki.
- 5.8 **Osoba Trzecia** - pracownik firmy zewnętrznej realizujący określone zadania na rzecz Spółki.
- 5.9 **Pracownik** – osoba, z którą pracodawca nawiązał stosunek pracy w rozumieniu art. 22 K.P., nie obejmuje osób wykonujących pracę na innej podstawie niż stosunek pracy.
- 5.10 **Procedura** – PROG 00041/A Procedura Ogólna zarządzania zdalnym dostępem do Sieci Korporacyjnej (VPN)
- 5.11 **Profil Zdalnego Dostępu VPN (Profil)** – zestaw uprawnień przyznanych określonej grupie Użytkowników w ramach korzystania ze zdalnego dostępu VPN, określający zakres docelowych usług osiągalnych z poziomu danego Użytkownika.
- 5.12 **Przełożony** – osoba posiadająca prawo do kierowania czynnościami służbowymi podlegających mu podwładnych w rozumieniu Regulaminu Organizacyjnego Spółki.
- 5.13 **Przetwarzanie Informacji** - jakiejkolwiek operacje wykonywane na informacji, w szczególności takie jak ich zbieranie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie, przesyłanie i usuwanie.
- 5.14 **Sieć Korporacyjna** - urządzenia komputerowe, oprogramowanie i okablowanie wraz z urządzeniami sieciowymi, umożliwiające gromadzenie, przetwarzanie oraz wymianę informacji.

- 5.15 **Spółka Grupy PGE, Spółka, Spółki** – podmiot / podmioty prawa handlowego wchodzące w skład Grupy PGE.
- 5.16 **System Teleinformatyczny (System)** - zespół środków technicznych wraz z oprogramowaniem tworzący logiczną i nierozrwalną całość wyodrębnioną ze względu na dostarczaną funkcjonalność przy założeniu, że głównym jego celem jest Przetwarzanie Informacji.
- 5.17 **Użytkownik** - osoba uprawniona do korzystania z Systemu Teleinformatycznego, użytkownikami mogą być Członkowie Organów Spółki, Pracownicy oraz Osoby Trzecie.
- 5.18 **Właściciel Profilu** - osoba w strukturze organizacyjnej Spółki sprawująca nadzór nad danym Profilem. Domyślnie jest to Kierownik Komórki organizacyjnej, w której wnioskowano o utworzenie Profilu.
- 5.19 **Wniosek** – formalne wystąpienie o podjęcie określonych działań w zakresie nadania, modyfikacji lub odebrania uprawnień do Usługi.
- 5.20 **Usługa** – część Systemu teleinformatycznego realizująca określoną funkcjonalność.
- 5.21 **Zatrudnienie** – umowa o pracę lub umowa cywilno-prawna zawarta pomiędzy osobą a Spółką.

VI REALIZACJA

1.1 ZASADY OGÓLNE

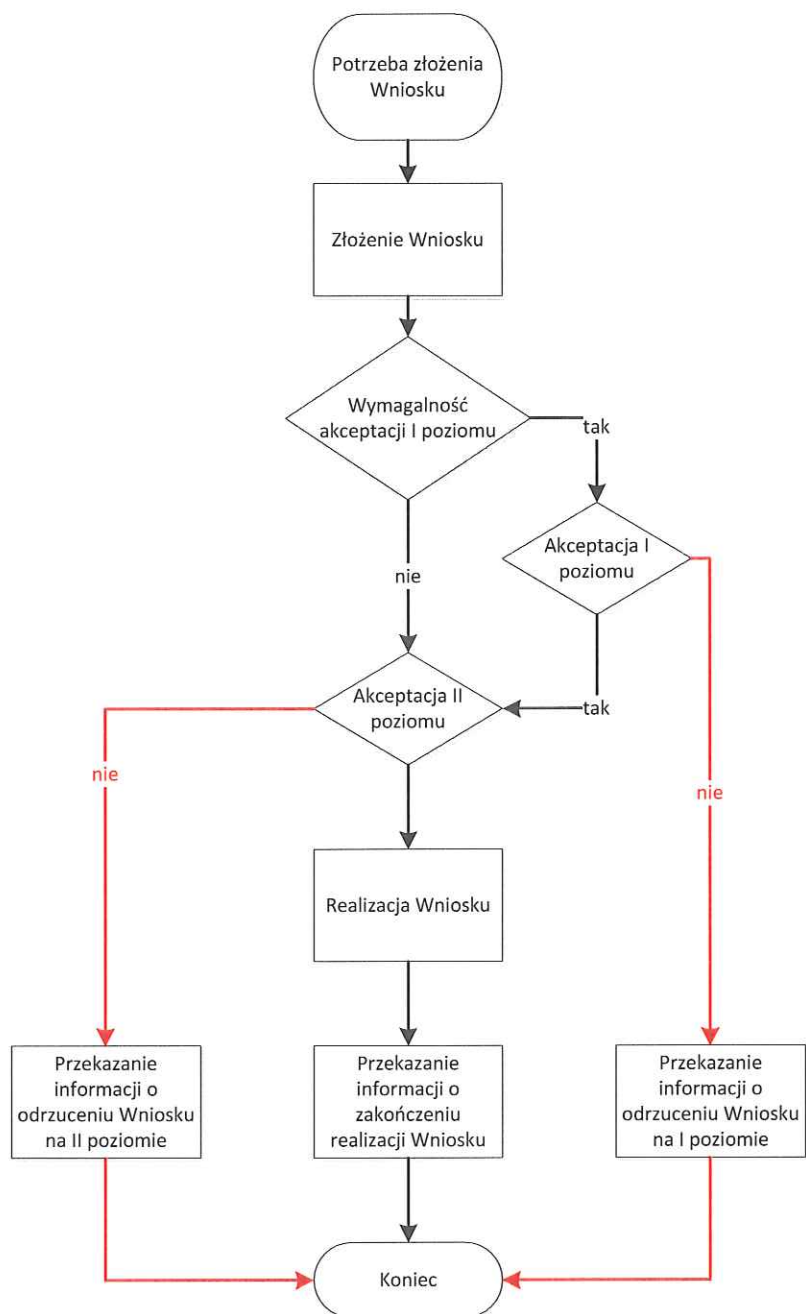
- 1.1.1 Uwierzytelnienie VPN odbywa się przez mechanizmy uwierzytelniania określone przez CUW ICT.
- 1.1.2 Użytkownicy potwierdzają znajomość Procedury oraz zobowiązanie do jej przestrzegania składając pisemne oświadczenie ([Załącznik 1](#)) do kierującego Komórką organizacyjną, w której są zatrudnieni. Kierujący komórką przekazuje oświadczenie do właściwej komórki lub Spółki odpowiedzialnej za obsługę kadrowo-płacową.
- 1.1.3 CUW ICT prowadzi ewidencję dostępów do Sieci Korporacyjnej z wykorzystaniem VPN. Ewidencja powinna w szczególności zawierać listę dostępów nadanych i odebranych oraz Profili uprawnień.
- 1.1.4 Uprawnienia dostępu zdalnego VPN oparte są na Profilach uprawnień.
- 1.1.5 Dostępy VPN typu serwisowego stanowią osobną grupę dostępów i przeznaczone są dla firm / osób, które na mocy odrębnej umowy administrują systemami. W umowach z firmami trzecimi, zawarte powinny być porozumienia, na mocy których dostępy VPN będą objęte procedurami zarządzania Użytkownikami.
- 1.1.6 W przypadku zestawienia zdalnego dostępu z wykorzystaniem VPN, przez tunel VPN musi być kierowany cały ruch sieciowy – również do sieci Internet.
- 1.1.7 Użytkownik jest odpowiedzialny za ochronę fizyczną sprzętu teleinformatycznego poza siedzibą Spółki. Sprzęt nie może być pozostawiany bez nadzoru w miejscach publicznych.
- 1.1.8 Sprzęt teleinformatyczny wykorzystywany do uzyskania zdalnego dostępu VPN musi spełniać warunki określone w PROG 00039 Procedura Ogólna bezpieczeństwa teleinformatycznego.
- 1.1.9 Użytkownik jest zobowiązany do zachowania należytej staranności w zakresie ochrony - poufność hasła, kluczy, certyfikatu lub innych danych poufnych wykorzystywanych do uwierzytelnienia w usłudze VPN.
- 1.1.10 Użytkownik ponosi pełną odpowiedzialność za nieautoryzowany dostęp do Sieci Korporacyjnej z wykorzystaniem VPN.
- 1.1.11 Po zakończeniu pracy zdalnej Użytkownik musi zamknąć sesję VPN.
- 1.1.12 Użytkownik jest zobowiązany do przestrzegania zasad bezpieczeństwa przyjętych w Spółce, w tym w szczególności określonych w PROG 00039 Procedura Ogólna bezpieczeństwa teleinformatycznego oraz PROG 00040 Procedura Ogólna zarządzania dostępem do podstawowych zasobów informatycznych Grupy PGE.
- 1.1.13 Wykorzystanie zdalnego dostępu VPN może być monitorowane pod kątem wykorzystania zgodnego z powyższymi zasadami.
- 1.1.14 W przypadku naruszenia powyższych zasad, dostęp do usługi VPN może być odebrany Użytkownikowi bez uprzedzenia.

1.2 ZARZĄDZANIE ZDALNYM DOSTĘPEM DO SIECI KORPORACYJNEJ Z WYKORZYSTANIEM VPN

1.2.1 Nadawanie, modyfikacja i odbieranie uprawnień

- 1.2.1.1 Zdalny dostęp do Sieci Korporacyjnej z wykorzystaniem VPN jest nadawany, modyfikowany i odbierany na podstawie Wniosków w Systemie OW dostępnych pod adresem <https://sd.gkpge.pl>.
- 1.2.1.2 W przypadku braku dostępu do Systemu OW dopuszcza się Wnioski papierowe ([Załącznik 2](#), [Załącznik 3](#)), które po zatwierdzeniu powinny zostać zeskanowane i przesłane na adres <https://sd.gkpge.pl>.
- 1.2.1.3 Wnioskodawca występuje z Wnioskiem o nadanie dostępu dla Pracownika gdy te uprawnienia przysługują z racji stanowiska i obowiązków służbowych Pracownika.

- 1.2.1.4 Wnioskodawca występuje z Wnioskiem o nadanie dostępu dla Osoby Trzeciej gdy te uprawnienia przysługują Osobie Trzeciej z racji działań realizowanych na rzecz Spółki.
- 1.2.1.5 Wnioskodawca występuje z Wnioskiem o nadanie dostępu dla Członka Organu Spółki gdy te uprawnienia przysługują z racji stanowiska i obowiązków służbowych Członka Organu Spółki.
- 1.2.1.6 Wnioskodawca występuje z Wnioskiem o modyfikację dostępu dla Pracownika w następujących sytuacjach:
 - a. zmiana stanowiska pracy,
 - b. zmiana obowiązków służbowych.
- 1.2.1.7 Wnioskodawca występuje z Wnioskiem o modyfikację dostępu dla Osoby Trzeciej gdy nastąpiła zmiana zakresu działań realizowanych przez Osobę Trzecią na rzecz Spółki.
- 1.2.1.8 Wnioskodawca występuje z Wnioskiem o modyfikację dostępu dla Członka Organu Spółki gdy nastąpiła zmiana zakresu działań realizowanych przez Członka Organu Spółki.
- 1.2.1.9 Wnioskodawca występuje z Wnioskiem o odebranie dostępu dla Pracownika w następujących sytuacjach:
 - a. rozwiązanie umowy o pracę,
 - b. zmiana obowiązków służbowych.
- 1.2.1.10 Wnioskodawca występuje z Wnioskiem o odebranie dostępu dla Osoby Trzeciej w następujących sytuacjach:
 - a. zakończenie realizacji działań na rzecz Spółki,
 - b. zmiana zakresu działań realizowanych przez Osobę Trzecią na rzecz Spółki.
- 1.2.1.11 Wnioskodawca występuje z Wnioskiem o odebranie uprawnień dla Członka Organu Spółki po odwołaniu Członka Organu Spółki .
- 1.2.1.12 Wnioskodawcą może być:
 - a. dla Pracownika – Przełożony, Nadzorca Dostępu,
 - b. dla Osoby Trzeciej - Opiekun Osoby Trzeciej, Nadzorca Dostępu,
 - c. dla Członka Organu Spółki - Kierownik Komórki organizacyjnej właściwej ds. obsługi władz Spółki, Nadzorca Dostępu.
- 1.2.1.13 W szczególności Wnioskodawcą może być sam Użytkownik lub inne osoby wyznaczone do wnioskowania o daną usługę. W takim przypadku wymagana jest akceptacja Wniosku:
 - a. dla Pracownika przez Przełożonego,
 - b. dla Osoby Trzeciej przez Opiekuna Osoby Trzeciej,
 - c. dla Członka Organu Spółki - Kierownika Komórki organizacyjnej właściwej ds. obsługi władz Spółki
- 1.2.1.14 Wnioskowanie przebiega według następującego schematu:



L.P.	Czynność	Odpowiedzialność za wykonanie czynności	Opis
Potrzeba nadania, modyfikacji lub odebrania uprawnień do zdalnego dostępu VPN			
1.	Złożenie Wniosku	Wnioskodawca	Osoba składająca Wniosek uzupełnia niezbędne dane dotyczące składanego Wniosku.
2.	Wymagalność akceptacji I poziomu		Akceptacja nie jest wymagana jeśli Wniosek został złożony dla Pracownika przez Przełożonego, dla Osoby Trzeciej przez jej Opiekuna Osoby Trzeciej, dla Członka Organu Spółki przez Kierownika Komórki organizacyjnej właściwej ds. obsługi władz Spółki lub przez Nadzorcę Dostępu.
3.	Akceptacja I poziomu	Przełożony, Opiekun Osoby Trzeciej, Kierownik Komórki organizacyjnej właściwej ds. obsługi władz	Przełożony, Opiekun Osoby Trzeciej, Kierownik Komórki organizacyjnej właściwej ds. obsługi władz Spółki jest informowany o potrzebie akceptacji Wniosku. Przełożony dla Pracownika, Opiekun Osoby Trzeciej dla Osoby Trzeciej, Kierownik Komórki organizacyjnej właściwej ds. obsługi władz Spółki dla Członka Organu Spółki akceptuje Wniosek lub odrzuca. Przed akceptacją Wniosku osoba akceptująca ma obowiązek upewnić się, że Użytkownik, któremu ma zostać nadany dostęp podpisał oświadczenie zgodne z <u>Załącz. 1</u> do niniejszej Procedury.
4.	Akceptacja II poziomu	Nadzorca Dostępu	Nadzorca Dostępu jest informowany o potrzebie akceptacji Wniosku, a następnie akceptuje go lub odrzuca.
5.	Realizacja Wniosku	Administrator	Administrator otrzymuje informację o potrzebie realizacji Wniosku i wykonuje czynności niezbędne do jego realizacji. W przypadku odbierania uprawnień Administrator ma obowiązek odebrania wszystkich uprawnień dla danego Użytkownika. Administrator aktualizuje ewidencję Dostępów zdalnych VPN.
6.	Przekazanie informacji o zakończeniu realizacji Wniosku	Administrator	W momencie skutecznego przekazania danych o wnioskowanych uprawnieniach, wnioskodawca oraz akceptujący informowani są o pozytywnym zakończeniu procesu.
7.	Przekazanie informacji o odrzuceniu Wniosku na I poziomie	Przełożony, Opiekun Osoby Trzeciej, Kierownik Komórki organizacyjnej właściwej ds. obsługi władz	Poinformowanie Wnioskodawcy o braku akceptacji I poziomu.
8.	Przekazanie informacji o odrzuceniu Wniosku na II poziomie	Nadzorca Dostępu	Poinformowanie Wnioskodawcy o braku akceptacji II poziomu.

1.2.1.15 Zdalny dostęp do Sieci Korporacyjnej z wykorzystaniem VPN dla Osób trzecich może być nadany jedynie na czas określony, nie dłuższy niż okres realizacji działań na rzecz Spółki.

1.2.1.16 Standardowy czas na akceptację I poziomu wynosi 14 dni. Po tym terminie Wniosek automatycznie jest odrzucany. Wnioskodawca jest informowany o braku akceptacji na I poziomie z powodu przeterminowania – nie podjęcia akcji przez akceptującego na I poziomie.

1.2.1.17 Standardowy czas na akceptację II poziomu wynosi 14 dni. Po tym terminie Wniosek automatycznie jest odrzucany. Wnioskodawca jest informowany o braku akceptacji na II poziomie z powodu przeterminowania – nie podjęcia akcji przez akceptującego na II poziomie.

1.2.1.18 Nadzorcą Dostępu jest

- dla Pracownika - Kierownik Komórki organizacyjnej w ramach której zatrudniony jest Pracownik,
- dla Osoby Trzeciej - Kierownik Komórki organizacyjnej, w ramach której osoba Trzecia realizuje swoje zadania,
- dla Członka Organu Spółki - Kierownik Komórki organizacyjnej właściwej ds. obsługi władz Spółki.

1.2.1.19 Jeśli Nadzorca Dostępu wystąpił jako akceptujący na I poziomie i jego akceptacja była pozytywna, to nie jest wymagana akceptacja na II poziomie.

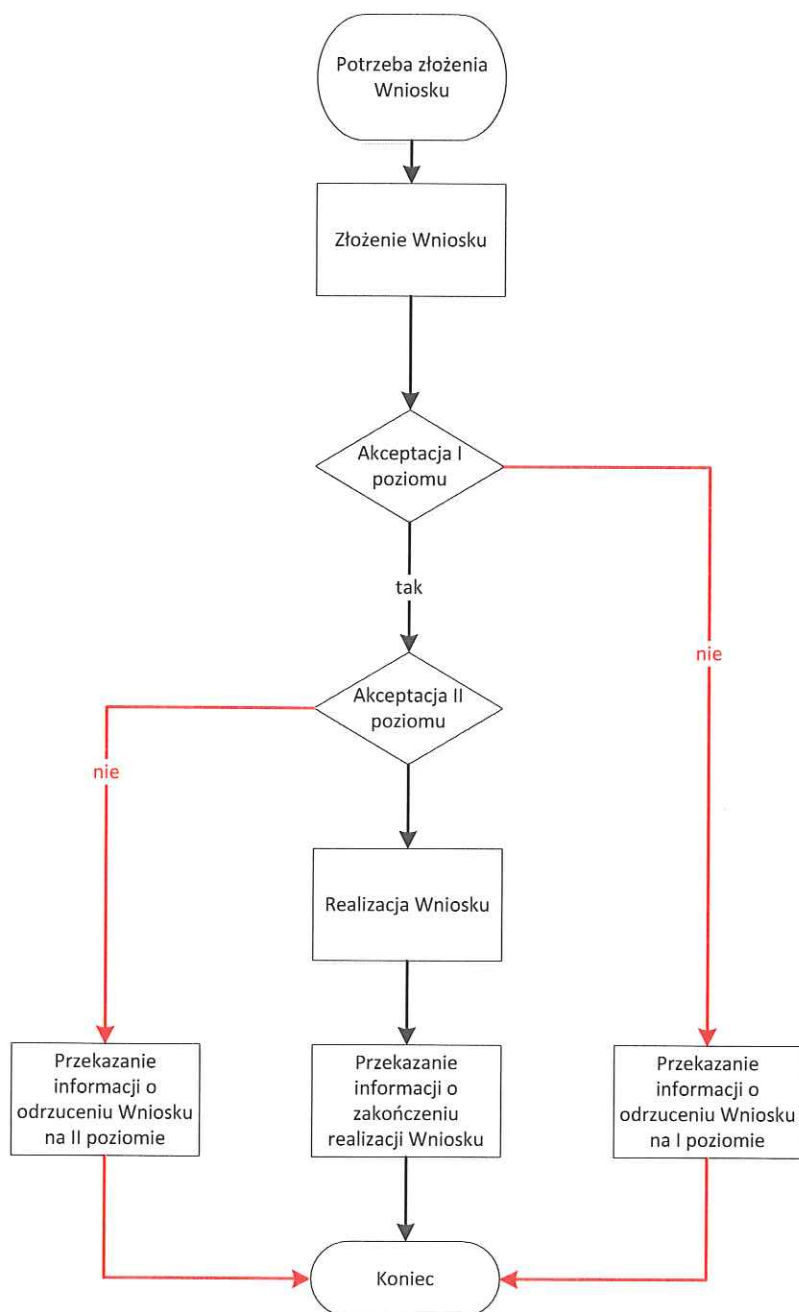
1.2.2 Przegląd uprawnień

- 1.2.2.1 Przegląd uprawnień zdalnego dostępu VPN powinien być rozumiany jako okresowa kontrola tego, czy Użytkownicy mają nadany taki zakres uprawnień, jaki wynika z wykonywanych obowiązków.
- 1.2.2.2 Przegląd uprawnień powinien być wykonywany co najmniej raz do roku oraz w przypadku istotnych zmian technologicznych lub organizacyjnych.
- 1.2.2.3 Za inicjowanie przeglądu uprawnień odpowiedzialny jest Nadzorca Dostępu, zaś nadzór nad terminowym wykonywaniem przeglądu sprawuje Kierownik Komórki organizacyjnej odpowiedzialnej za bezpieczeństwo teleinformatyczne w danej Spółce.
- 1.2.2.4 Po rozpoczęciu przeglądu Administrator tworzy listę Użytkowników i uprawnień. Następnie lista ta przekazywana jest odpowiednim Przełożonym, Opiekunom Osób Trzecich oraz Kierownikowi Komórki organizacyjnej właściwej ds. obsługi władz Spółki.
- 1.2.2.5 Przełożeni, Opiekunowie Osób trzecich oraz Kierownik Komórki organizacyjnej właściwej ds. obsługi władz Spółki weryfikują w terminie 14 dni, czy wskazane uprawnienia w kontekście zadań biznesowych i odpowiedzialności posiadających je Użytkowników są zasadne.
- 1.2.2.6 Uprawnienia niepotwierdzone są przez Administratora odbierane.
- 1.2.2.7 Po odebraniu uprawnień Użytkownikowi, Administrator jest odpowiedzialny za poinformowanie o tym jego Przełożonego, Opiekuna Osoby Trzeciej lub Kierownika Komórki organizacyjnej właściwej ds. obsługi władz Spółki.
- 1.2.2.8 Po wykonaniu przeglądu uprawnień, Administrator jest zobowiązany do przekazania raportu podsumowującego Kierownikowi Komórki organizacyjnej odpowiedzialnej za bezpieczeństwo teleinformatyczne w danej Spółce.

1.3 PROFILE UPRAWNIEŃ ZDALNEGO DOSTĘPU VPN

1.3.1 Zarządzanie profilami Zdalnego Dostępu VPN

- 1.3.1.1 Profile Zdalnego Dostępu VPN są tworzone, modyfikowane, usuwane na podstawie Wniosków w Systemie OW dostępnych pod adresem <https://sd.gkpge.pl>.
- 1.3.1.2 W przypadku braku dostępu do Systemu OW dopuszcza się Wnioski papierowe ([Załącznik 4](#), [Załącznik 5](#)), które po zatwierdzeniu powinny zostać zeskanowane i przesłane na adres <https://sd.gkpge.pl>.
- 1.3.1.3 Wnioskodawca występuje z Wnioskiem o utworzenie Profilu Zdalnego Dostępu VPN, gdy jest to uzasadnione obowiązkami służbowymi danej grupy Pracowników, a Profil o analogicznym poziomie uprawnień nie istnieje.
- 1.3.1.4 Wnioskodawca występuje z Wnioskiem o modyfikację Profilu Zdalnego Dostępu VPN, gdy obowiązki służbowe grupy Pracowników wykorzystującej dany profil ulegną zmianie.
- 1.3.1.5 Wnioskodawca występuje z Wnioskiem o usunięcie Profilu Zdalnego Dostępu VPN, gdy dany Profil Zdalnego Dostępu VPN nie jest wykorzystywany przez żadnego Pracownika.
- 1.3.1.6 Wnioskodawcą może być każdy Pracownik.
- 1.3.1.7 Wnioskowanie przebiega według następującego schematu:



L.P.	Czynność	Odpowiedzialność za wykonanie czynności	Opis
Potrzeba nadania, modyfikacji lub usunięcia Profilu Zdalnego Dostępu VPN			
1.	Złożenie Wniosku	Wnioskodawca	Osoba składająca Wniosek uzupełnia niezbędne dane dotyczące składanego Wniosku.
3.	Akceptacja I poziomu	Kierownik Komórki organizacyjnej wnioskodawcy lub osoba przez niego upoważniona	Kierownik Komórki organizacyjnej wnioskodawcy jest informowany o potrzebie akceptacji Wniosku, który następnie akceptuje wniosek lub odrzuca.
4.	Akceptacja II poziomu	Dyrektor Departamentu Bezpieczeństwa i Ciągłości Biznesowej IT w PGE Systemy S.A. lub osoba przez niego upoważniona	Dyrektor Departamentu Bezpieczeństwa i Ciągłości Biznesowej IT w PGE Systemy S.A. lub osoba przez niego wyznaczona jest informowany o potrzebie akceptacji Wniosku, a następnie akceptuje go lub odrzuca.
5.	Realizacja Wniosku	Administrator	Administrator otrzymuje informację o potrzebie realizacji Wniosku i wykonuje czynności niezbędne do jego realizacji. Administrator aktualizuje listę Profili (Załącznik 4 do niniejszej procedury).
6.	Przekazanie informacji o zakończeniu realizacji Wniosku	Administrator	W momencie skutecznego przekazania danych o wnioskowanych uprawnieniach, wnioskodawca oraz akceptujący oraz Właściciel Profilu informowani są o pozytywnym zakończeniu procesu.
7.	Przekazanie informacji o odrzuceniu Wniosku na I poziomie	Kierownik Komórki organizacyjnej wnioskodawcy lub osoba przez niego upoważniona	Poinformowanie wnioskodawcy o braku akceptacji I poziomu.
8.	Przekazanie informacji o odrzuceniu Wniosku na II poziomie	Kierownik Komórki organizacyjnej odpowiedzialnej za bezpieczeństwo lub osoba przez niego upoważniona	Poinformowanie wnioskodawcy o braku akceptacji II poziomu.

1.3.1.8 Standardowy czas na akceptację I poziomu wynosi 7 dni. Po tym terminie Wniosek automatycznie jest odrzucany. Wnioskodawca jest informowany o braku akceptacji na I poziomie z powodu przeterminowania – nie podjęcia akcji przez akceptującego na I poziomie.

1.3.1.9 Standardowy czas na akceptację II poziomu wynosi 7 dni. Po tym terminie Wniosek automatycznie jest odrzucany. Wnioskodawca jest informowany o braku akceptacji na II poziomie z powodu przeterminowania – nie podjęcia akcji przez akceptującego na II poziomie.

1.3.1.10 Jeśli we Wniosku nie wskazano inaczej, Właścicielem Profilu jest Kierownik Komórki organizacyjnej Pracownika składającego Wniosek.

1.4 PRZEGLĄD PROFILI UPRAWNIEŃ

1.4.1 Przegląd Profili uprawnień powinien być inicjowany przez Właścicieli poszczególnych Profili co najmniej raz do roku oraz w przypadku istotnych zmian technologicznych lub organizacyjnych.

1.4.2 Właściciel Profilu aktualizuje zakres uprawnień dostępnych w ramach Profilu zgodnie z procedurą modyfikacji Profilu.

1.4.3 Za każdym razem przy zakończeniu przeglądu, jego podsumowanie i wynik przesyłany jest do Dyrektora Departamentu Bezpieczeństwa i Ciągłości Biznesowej IT w PGE Systemy S.A., a lista Profili jest aktualizowana.

1.5 POSTANOWIENIA KOŃCOWE

1.1.1 Systemy Teleinformatyczne oraz dane w nich przetwarzane muszą być zabezpieczone zgodnie z wytycznymi zawartymi w PROG 00039 Procedura Ogólna bezpieczeństwa teleinformatycznego. Zapisy objęte treścią niniejszej Procedury stanowią uszczegółowienie PROG 00039 Procedura Ogólna bezpieczeństwa teleinformatycznego.

- 1.1.2 W zakresie nie objętym niniejszą Procedurą lub innymi regulacjami zawartymi w aktach normatywnych Spółki, należy postępować zgodnie z interesem Spółki, kierując się wiedzą oraz najlepszymi praktykami z dochowaniem należytej staranności we wszystkich podejmowanych działaniach.
- 1.1.3 Wszelkie zmiany w treści Procedury są wprowadzane zgodnie z zasadami obowiązującymi w Spółkach Grupy PGE.
- 1.1.4 Odstępstwa od procedury w zakresie punktu 6.2 akceptuje Dyrektor Departamentu Strategii IT lub Dyrektor Departamentu Bezpieczeństwa i Ciągłości Biznesowej w PGE Systemy S.A.
- 1.1.5 Za modyfikację załączników odpowiada Dyrektor Departamentu Strategii IT Grupy Kapitałowej PGE bez konieczności ponownego zatwierdzania Procedury.