



Polskie Porty Lotnicze
Polish Airports

PROCEDURA

DOSTĘP DO ZASOBÓW SIECI INFORMATYCZNEJ PPL S.A. POPRZEZ VPN

PS-VPN-01

	Nazwa stanowiska	Data, pieczęćka, podpis
Dokument zatwierdził:	Prezes Zarządu Polskich Portów Lotniczych S.A.	CZŁONEK ZARZĄDU Polskie Porty Lotnicze S.A. <i>Monika Niewczas</i> 23.10.23
Właściciel dokumentu:	Dyrektor Biura Informatyki i Systemów Bezpieczeństwa	
Administrator dokumentu:	Główny Specjalista/Specjalista w Zespole Zarządzania Infrastrukturą Sieciową	



SPIS TREŚCI

1.	CZĘŚĆ OGÓLNA	4
1.1.	Cel i zakres stosowania dokumentu	4
1.2.	Postanowienia ogólne	4
2.	OPIS DZIAŁAŃ	5
2.1.	Sporządzenie wniosku o dostęp do VPN	5
2.1.1.	Wypełnianie wniosku	5
2.1.2.	Weryfikacja wniosku przez bezpośredniego przełożonego Wnioskodawcy / Administratora biznesowego	6
2.1.3.	Zarejestrowanie zgłoszenia z wnioskiem	6
2.2.	Weryfikacja zarejestrowanego wniosku o dostęp do VPN	6
2.2.1.	Ocena wniosku przez odpowiedzialnego za udostępniane zasoby	6
2.2.2.	Ocena wniosku przez Dział Cyberbezpieczeństwa	6
2.3.	Realizacja dostępu VPN po zatwierdzeniu wniosku	7
2.3.1.	Konfiguracja urządzeń	7
2.3.2.	Przekazanie dostępu VPN	7
2.3.3.	Zatwierdzenie i przekazanie Listy dostępowej	7
2.3.4.	Prowadzenie dokumentacji	7
2.3.5.	Aktualizacja Listy dostępowej	7
2.4.	Postępowanie przy nawiązywaniu połączenia RA VPN	8
2.4.1.	Udzielanie dostępu dla użytkowników VPN	8
2.4.1.1.	Dla Pracownika/współpracownika PPL S.A. (RA VPN):	8
2.4.1.2.	Dla podmiotu zewnętrznego (RA VPN)	8



2.5.	Zakończenie korzystania z dostępu VPN	9
2.5.1.	Zakończenie korzystania z dostępu VPN	9
2.5.2.	Usunięcie konta użytkownika VPN	9
2.5.3.	Usunięcie użytkownika VPN z Listy dostępowej	9
3.	POSTĘPOWANIE W SYTUACJACH AWARYJNYCH	9
4.	DEFINICJE I SKRÓTY	10
4.1.	Definicje	10
4.2.	Skróty	12
5.	WYKAZ DOKUMENTÓW ZWIĄZANYCH	12
6.	WYKAZ UŻYTKOWNIKÓW DOKUMENTU	12
7.	WYKAZ ZAŁĄCZNIKÓW	12



1. CZĘŚĆ OGÓLNA

1.1. Cel i zakres stosowania dokumentu

1. Celem niniejszej procedury jest przedstawienie procesu uzyskiwania dostępu do zasobów informatycznych PPL S.A. poprzez szyfrowane łącze VPN.
2. Procedura obowiązuje wszystkie komórki organizacyjne PPL S.A. i podmioty zewnętrzne, które ze względu na świadczoną usługę wymagają dostępu do systemów informatycznych PPL S.A. z wykorzystaniem szyfrowanego połączenia VPN. Procedura dotyczy w szczególności obszarów związanych z zachowaniem ciągłości działania portu lotniczego (np. dostęp dla administratorów spoza sieci informatycznej PPL S.A., podmiotów zewnętrznych serwisujących systemy informatyczne itp.).

1.2. Postanowienia ogólne

1. W celu uzyskania dostępu VPN do sieci PPL S.A. (dającego możliwość podłączenia do określonego systemu IT) konieczne jest spełnienie wymagań opisanych w niniejszej procedurze. Powyższe nie dotyczy z wyłączeniem podstawowych dostępu uzyskanych na podstawie „[Wniosku o dostęp do zasobów teleinformatycznych PPL](#)” (F01-RE-IT-01).
2. Dostęp do systemów teleinformatycznych nadawany jest zgodnie z [Regulaminem „Wykorzystywanie zasobów teleinformatycznych”](#) (RE-IT-01).
3. Wnioskowany zakres dostępu VPN do systemów informatycznych w sieci PPL S.A. musi być zgodny z zakresem upoważnienia do dostępu i przetwarzania danych osobowych. Odpowiedzialność za zapewnienie zgodności w tym zakresie ponosi Przełożony Wnioskodawcy wnioskującego o dostęp do zasobów poprzez VPN.
4. Rozróżnia się trzy rodzaje dostępu VPN:
 - 1) dla pracowników/współpracowników PPL S.A. – dostęp typu Remote Access VPN (RA VPN);
 - 2) dla podmiotów zewnętrznych – dostęp typu:
 - a) Remote Access VPN (RA VPN),
 - b) Site-to-Site VPN (S2S VPN).

2. OPIS DZIAŁAŃ

2.1. Sporządzenie wniosku o dostęp do VPN

Oceny i akceptacji wniosku na każdym z poniższych etapów dokonuje osoba wskazana jako odpowiedzialna. W przypadku braku akceptacji (decyzja odmowna) następuje odrzucenie zgłoszenia wraz z uzasadnieniem.

2.1.1. Wypełnianie wniosku

1. Wniosek o dostęp VPN do określonego(-ych) systemu(-ów) / sieci stanowi formularz [„Wniosek o dostęp VPN” \(F01-PS-VPN-01\)](#).
2. Wnioski wypełniane są w następującym zakresie:
 - 1) wniosek o RA VPN (Remote Access VPN) dla pracownika/współpracownika PPL S.A. wypełnia osoba zainteresowana lub Przełożony Wnioskodawcy;
 - 2) wniosek o S2S VPN (Site-to-Site VPN) lub RA VPN (Remote Access VPN) dla podmiotu zewnętrznego wypełnia w jego imieniu Administrator Biznesowy usługi w porozumieniu z Administratorem Technicznym.
3. Wnioskodawca ustala z Administratorem Technicznym informacje konieczne do prawidłowego wypełnienia danych we wniosku: szczegółowe określenie zasobów, które mają być dostępne poprzez VPN dla użytkownika (sieć, serwer, aplikacje, protokoły). Informacje dotyczące poprawnego wypełniania [„Wniosku o dostęp VPN” \(F01-PS-VPN-01\)](#) zawarte są w [„Instrukcji wypełniania wniosku VPN” \(Z01-PS-VPN-01\)](#).
4. Dla dostępu typu RA VPN dla podmiotów zewnętrznych, gdy wniosek dotyczy grupy pracowników, dodatkowo wypełniania jest [„Lista dostępowa” \(F02-PS-VPN-01\)](#). Lista zawiera następujące dane:
 - 1) imię i nazwisko Użytkownika VPN,
 - 2) numer telefonu Użytkownika VPN,
 - 3) kod identyfikujący Użytkownika VPN – identyfikator nadany przez Administratora Biznesowego w porozumieniu z Administratorem VPN.
5. Wnioskodawca jest odpowiedzialny za prawidłowe wypełnienie wniosku zgodnie z danymi wynikającymi z aktualnych dokumentów stanowiących podstawę do wypełnienia wniosku.
6. Wnioskodawca jest uprawniony do korzystania z informacji uzyskanych od Administratora Technicznego i Administratora VPN w celu prawidłowego wypełnienia Wniosku.

2.1.2. Weryfikacja wniosku przez bezpośredniego przełożonego Wnioskodawcy / Administratora biznesowego

Po wypełnieniu Wniosku następuje ocena potrzeby biznesowej uzyskania dostępu do zasobów poprzez VPN oraz weryfikacja kompletności Wniosku. Prawidłowo wypełniony Wniosek podlega akceptacji przez bezpośredniego przełożonego lub Administratora Biznesowego.

2.1.3. Zarejestrowanie zgłoszenia z wnioskiem

Wnioskodawca rejestruje Wniosek w ITSM, z ewentualnym wsparciem COT, poprzez załączenie do zgłoszenia Wniosku wraz z Listą dostępową, jeżeli wymagane jest jej wypełnienie. Zgłoszenie w ITSM podlega kolejnym weryfikacjom.

2.2. Weryfikacja zarejestrowanego wniosku o dostęp do VPN

2.2.1. Ocena wniosku przez odpowiedzialnego za udostępniane zasoby

1. Po rejestracji Wniosku następuje weryfikacja konieczności uzyskania dostępu do zasobów i ewentualna akceptacja Wniosku przez osobę odpowiedzialną za udostępniane zasoby. Weryfikacja dotyczy:
 - 1) zasobu do którego dostęp jest wnioskowany (pkt. 6 Wniosku);
 - 2) użytkownika lub Listy dostępowej (pkt. 8 Wniosku);
 - 3) okresu, na jaki niezbędny jest dostęp (pkt. 5 Wniosku).
2. Podstawą ww. danych są dokumenty, za których legalność, zgodność i aktualność odpowiedzialny jest bezpośredni przełożony Wnioskodawcy lub Administrator Biznesowy.

2.2.2. Ocena wniosku przez Dział Cyberbezpieczeństwa

Zaakceptowany przez wszystkie osoby biorące udział w procesie zatwierdzania Wniosek o dostęp VPN trafia do Działu Cyberbezpieczeństwa. Pracownik Zespołu Cyberbezpieczeństwa weryfikuje kompletność Wniosku i zakres wnioskowanego dostępu pod kątem cyberbezpieczeństwa oraz dokonuje zatwierdzenia lub odrzucenia Wniosku.

2.3. Realizacja dostępu VPN po zatwierdzeniu wniosku

2.3.1. Konfiguracja urządzeń

Konfiguracja VPN realizowana jest przez Administratora VPN zgodnie z Wnioskiem załączonym do zgłoszenia w ITSM. W razie wystąpienia takiej konieczności, Administrator VPN uzgadnia szczegóły techniczne z odpowiednim Administratorem Technicznym.

2.3.2. Przekazanie dostępu VPN

1. RA VPN dla pracownika/współpracownika PPL S.A. – dodatkowe uwierzytelnienie za pomocą aplikacji DUO.
2. RA VPN dla pracownika podmiotu zewnętrznego – część statyczna haseł użytkowników z Listy dostępowej wraz z samą Listą oraz sposobem uwierzytelniania przekazywana jest podmiotowi zewnętrznemu przez Administratora Biznesowego
3. S2S VPN – dokument zawierający parametry połączenia przekazywany jest podmiotowi zewnętrznemu przez Administratora VPN.

2.3.3. Zatwierdzenie i przekazanie Listy dostępowej

Administrator VPN zatwierdza i przekazuje Listę dostępową do COT.

2.3.4. Prowadzenie dokumentacji

Za prowadzenie pełnej dokumentacji procesu opisanego w niniejszej procedurze, przechowywanie dokumentacji oraz dbałość o aktualność danych odpowiada Administrator VPN.

2.3.5. Aktualizacja Listy dostępowej

1. Administrator Biznesowy aktualizuje Listę dostępową w przypadku konieczności wprowadzenia zmian na Liście dostępowej. Zmiany mogą dotyczyć dodania dodatkowych osób lub wykreślenia osób znajdujących się na tej Liście.
2. W przypadku konieczności aktualizacji Listy dostępowej Administrator Biznesowy aktualizuje formularz [„Lista dostępowa” \(F02-PS-VPN-01\)](#) i przekazuje COT w celu zarejestrowania zgłoszenia dla Administratora VPN.
3. Wskazanie dodatkowych osób na Liście dostępowej dla podmiotu zewnętrznego, dla którego wniosek o VPN jest aktywny nie wymaga ponownego procedowania Wniosku.



2.4. Postępowanie przy nawiązywaniu połączenia RA VPN

2.4.1. Udzielanie dostępu dla użytkowników VPN

2.4.1.1. Dla Pracownika/współpracownika PPL S.A. (RA VPN)

1. Użytkownik VPN GP loguje się do sieci PPL S.A. za pomocą aplikacji „GlobalProtect” i konta domenowego poprzez komputer służbowy.
2. Na sprzęcie komputerowym użytkownika musi być zainstalowany odpowiedni certyfikat pozwalający na dostęp do sieci PPL S.A., a na smartfonie służbowym aplikacja DUO w celu dokonania dwuetapowego uwierzytelnienia.
3. Po poprawnym zalogowaniu się na komputerze służbowym do aplikacji „GlobalProtect” użytkownik VPN otrzymuje powiadomienie z aplikacji DUO na służbowym telefonie, w którym przez metodę PUSH potwierdza chęć dostępu do VPN.

2.4.1.2. Dla podmiotu zewnętrznego (RA VPN)

1. Użytkownik VPN kontaktuje się z COT (tel. +48 603 958 057 lub +48 22 650 23 80) w celu uzyskania dostępu VPN do zasobów PPL S.A..
2. Użytkownik VPN identyfikuje się imieniem i nazwiskiem oraz indywidualnym kodem.
3. COT weryfikuje powyższe dane, a także numer telefonu, z którego telefonuje Użytkownik VPN, na Liście dostępowej. W przypadku braku możliwości weryfikacji numeru telefonu dzwoniącego, pracownik COT przerywa połączenie, a następnie oddzwania na numer telefonu podany do danego Użytkownika VPN na Liście dostępowej.
4. Po poprawnej weryfikacji Użytkownika VPN, COT przekazuje Użytkownikowi VPN Token.
5. Użytkownik VPN potwierdza, że połączenie VPN do zasobów wewnętrznych PPL S.A. zostało nawiązane.
6. COT odnotowuje fakt połączenia w [„Formularzu rejestracyjnym dostępu VPN konsultantów firm zewnętrznych” \(F03-PS-VPN-01\)](#).

2.5. Zakończenie korzystania z dostępu VPN

2.5.1. Zakończenie korzystania z dostępu VPN

Zakończenie korzystania z dostępu VPN na podstawie danych wynikających z Wniosku o dostęp VPN następuje z datą wskazaną we Wniosku. W przypadku zaistnienia okoliczności, w wyniku których konieczne jest odebranie uprawnień Użytkownikowi VPN przed datą wygaśnięcia Wniosku, Administrator Biznesowy lub przełożony Wnioskodawcy niezwłocznie przekazuje stosowną informację pracownikowi COT w celu zarejestrowania zgłoszenia dla Administratora VPN.

2.5.2. Usunięcie konta użytkownika VPN

W przypadku zaistnienia okoliczności, w wyniku których konieczne jest usunięcie konta użytkownika VPN i/lub blokady użytkownika, Administrator Biznesowy lub Administrator VPN (w zależności od okoliczności powodujących usunięcie/blokadę) informuje COT o konieczności usunięcia użytkownika z Listy dostępowej.

2.5.3. Usunięcie użytkownika VPN z Listy dostępowej

Administrator Biznesowy usuwa użytkownika z Listy dostępowej i przekazuje aktualną listę do COT oraz Administratora VPN za pomocą systemu ITSM.

3. POSTĘPOWANIE W SYTUACJACH AWARYJNYCH

W sytuacjach awaryjnych, wymagających natychmiastowych działań związanych z bezpieczeństwem lub ciągłością działania PPL S.A., decyzję o udostępnieniu, modyfikacji lub odebraniu dostępu VPN może podjąć Dyrektor Biura Informatyki i Systemów Bezpieczeństwa lub Kierownik Działu Cyberbezpieczeństwa.

4. DEFINICJE I SKRÓTY

4.1. Definicje

Administrator Biznesowy	Osoba odpowiedzialna za współpracę z Użytkownikiem VPN. Definicja własna TIIIEI
Administrator Techniczny	Osoba odpowiedzialna za dany zasób, do którego konieczne jest udzielenie dostępu VPN. Definicja własna TIIIEI
Administrator VPN	Pracownik Zespołu Zarządzania Infrastrukturą Sieciową (TIIIEI) odpowiedzialny za zarządzanie dostępem do zasobów sieci informacyjnej PPL S.A. przez VPN. Definicja własna TIIIEI
Aplikacja DUO	Aplikacja służąca do MFA (Uwierzytelnianie wieloskładnikowe). Definicja własna TIIIEI
Aplikacja MFA	Aplikacja zainstalowana na telefonach służbowych pracowników/ współpracowników PPL S.A. pozwalająca dokonywać autoryzacji przy logowaniu się do VPN. Definicja własna TIIIEI
Dostęp poprzez PUSH	Sposób uwierzytelnienia w Aplikacji MFA umożliwiający dostęp do VPN. Definicja własna TIIIEI
GlobalProtect	Aplikacja komputerowa, klient firmy VPN firmy Palo Alto Networks. Definicja własna TIIIEI
Hasło Użytkownika	Hasło ustawiane przez Użytkownika VPN podczas pierwszego logowania. Definicja własna TIIIEI
ITSM	Information Technology Service Management czyli system informatyczny wspomagający wszystkie działania związane z zarządzaniem usługami informatycznymi (IT) w przedsiębiorstwie. Definicja własna TIIIEI
Kod dostępowy	Hasło Użytkownika łącznie z Tokenem wprowadzane przez Użytkownika VPN w oknie logowania połączenia VPN. Definicja własna TIIIEI

Osoba Odpowiedzialna za udostępnianie zasoby	<p>Osoba odpowiedzialna biznesowo oraz podejmująca decyzję o udostępnieniu zasobów, w tym w szczególności za obszar merytoryczny udostępniany poprzez dostęp VPN do zasobów w sieci PPL S.A..</p> <p>Definicja własna TIIEI</p>
Podmiot zewnętrzny	<p>Podmiot zewnętrzny świadczący usługi na rzecz PPL S.A., posiadający podpisaną umowę na świadczenie usług wraz z dostępem zdalnym, której pracownik będzie uzyskiwał dostęp poprzez VPN do określonego systemu PPL S.A..</p> <p>Definicja własna TIIEI</p>
Pracownik/ Współpracownik PPL S.A.	<p>Pracownik - osoba zatrudniona przez Polskie Porty Lotnicze na podstawie umowy o pracę;</p> <p>Współpracownik – osoba związana z PPL S.A. umową na osobiste świadczenie usług na podstawie umowy B2B, umowy zlecenie, umowy o dzieło.</p> <p>Definicja własna TIIEI</p>
Przełożony Wnioskodawcy	<p>Przełożony, akceptujący dane wprowadzone we Wniosku z uwzględnieniem legalności, zgodności i aktualności tych danych zgodnie z obowiązującym w PPL S.A. Regulaminem Organizacyjnym (RE-ORGANIZACYJNY-01).</p> <p>Definicja własna TIIEI</p>
RA VPN	<p>Remote Access VPN – rodzaj dostępu zdalnego nawiązywany tymczasowo pomiędzy użytkownikiem, a siecią lokalną PPL S.A..</p> <p>Definicja własna TIIEI</p>
S2S VPN	<p>Site-to-site VPN – rodzaj dostępu zdalnego nawiązywany na stałe pomiędzy siecią lokalną PPL S.A., a siecią lokalną Podmiotu Zewnętrznego.</p> <p>Definicja własna TIIEI</p>
Token	<p>9 cyfrowy kod generowany przez aplikację MFA (Uwierzytelnianie wieloskładnikowe).</p> <p>Definicja własna TIIEI</p>
Użytkownik VPN	<p>Pracownik/współpracownik PPL S.A. lub podmiot zewnętrzny, który będzie łączył się z wybranym systemem PPL S.A. poprzez VPN.</p> <p>Definicja własna TIIEI</p>



VPN	Zdalny, szyfrowany kanał dostępowy do zasobów informatycznych PPL S.A.. Definicja własna TII EI
Wnioskodawca	Pracownik/współpracownik PPL S.A. (Użytkownik lub Administrator Biznesowy) składający wniosek o dostęp VPN. Definicja własna TII EI
Zasób	Określona lokalizacja w sieci informatycznej pozwalająca na dostęp do określonych systemów informatycznych, aplikacji, plików, serwerów itp.. Definicja własna TII EI

4.2. Skróty

COT	Centrum Operacyjne Teleinformatyki
PPL S.A.	Przedsiębiorstwo Państwowe „Porty Lotnicze”
TII EI	Zespół Zarządzania Infrastrukturą Sieciową

5. WYKAZ DOKUMENTÓW ZWIĄZANYCH

1. [Regulamin „Wykorzystywanie zasobów teleinformatycznych” \(RE-IT-01\).](#)

6. WYKAZ UŻYTKOWNIKÓW DOKUMENTU

1.	Komórki organizacyjne PPL S.A.	Wszystkie komórki organizacyjne PPL S.A.
2.	Podmioty zewnętrzne	TAK – dostawcy usług - konsultanci

7. WYKAZ ZAŁĄCZNIKÓW

Załącznik nr 1 - [Z01-PS-VPN-01 Instrukcja wypełniania wniosku VPN](#)

Załącznik nr 2 - [F01-PS-VPN-01 Wniosek o dostęp VPN](#)

Załącznik nr 3 - [F02-PS-VPN-01 Lista dostępową](#)

Załącznik nr 4 - [F03-PS-VPN-01 Formularz rejestracyjny dostępu VPN konsultantów podmiotów zewnętrznych](#)