

Załącznik nr 11 do umowy nrz dnia

Formularze

Spis formularzy:

1. **Miesięczny protokół odbioru realizacji przedmiotu Umowy**
2. **Protokół odbioru Nowej wersji Systemu**
3. **Raport z testowania Nowej wersji Systemu**
4. **Wniosek o dostęp do zasobów infrastruktury techniczno-systemowej Ministerstwa Sprawiedliwości (ITS MS)**
5. **Załącznik nr 1 do Wniosku o dostęp do zasobów infrastruktury techniczno-systemowej Ministerstwa Sprawiedliwości (ITS MS)**
6. **Protokół odbioru Dokumentacji Systemu**

1. Miesięczny protokół odbioru realizacji przedmiotu Umowy:

Formularz protokołu miesięcznego odbioru realizacji przedmiotu Umowy

----- Wypełnia Wykonawca -----
System: **Wersja:**
Nazwa firmy:
Imię i nazwisko: **Data:** - -

zgłasza do odbioru usługi określone w § 2 ust. 1 Umowy za miesiąc:
w zakresie:

pkt 1); pkt 2); pkt 3); inne:
(niepotrzebne skreślić)

Poziom dostępności Systemu uzyskany z pomiaru [%]:

Załączniki do protokołu:

- raporty: m.in. poziomu dostępności Systemu, Zgłoszeń za usługi określone w § 2 ust. 1 pkt 1) lit. a-e, Zgłoszeń za usługi określone w § 2 ust. 1 pkt 2), Zgłoszeń za usługi określone w § 2 ust. 1 pkt 3), inne.
- inne protokoły: m.in. Protokół odbioru Nowej wersji Systemu z załączonym raportem z testowania Nowej wersji Systemu, Protokół odbioru szkoleń, Ankiety szkoleń, , inne.

Uwagi:

Podpis**
(Kierownik Projektu -
Wykonawcy)
**bezwzględnie wymagany
odrębny podpis +
pieczęć

----- Wypełnia DIRS -----
Departament Informatyzacji i Rejestrów Sądowych

Imię i nazwisko: **Data:** - -

dokonał odbioru usług określonych w § 2 ust. 1 za miesiąc: ,
w zakresie: pkt 1)

Decyzja: **nie dotyczy** ☐ **pozytywna** ☐ **negatywna** ☐

Uwagi odbierającego:

Zestawienie kar umownych: [Podstawa prawna z Umowy/Ilość/jednostka kary] – np.

Podstawa prawna z Umowy	ilość	jednostka kary
§ ... ust. ... pkt ... Umowy	...	9-ciogodzinne okresy opóźnienia
§ ... ust. ... pkt ... Umowy	...	24-godzinny okres opóźnienia
§ ust.... Umowy	...	uchybie

w zakresie: pkt 2)

Decyzja: **nie dotyczy** ☐ **pozytywna** ☐ **negatywna** ☐

Uwagi odbierającego:

Zestawienie kar umownych:

w zakresie: pkt 3)

Decyzja: *nie dotyczy* ☐ *pozytywna* ☐ *negatywna* ☐

Uwagi odbierającego:

Zestawienie kar umownych:

w zakresie innych usług realizowanych w ramach Umowy:

Decyzja: *nie dotyczy* ☐ *pozytywna* ☐ *negatywna* ☐

Uwagi odbierającego:

Zestawienie kar umownych:

Sporządzono w 4 jednobrzmiących egzemplarzach: 1 dla Wykonawcy, 3 dla Zamawiającego.

Akceptacja*
(Kierownik Projektu/Opiekun umowy
po stronie Zamawiającego)
**bezwzględnie wymagany odręczny
podpis + pieczęć

2. Protokół odbioru Nowej wersji Systemu:

Protokół odbioru Nowej wersji Systemu

1. Data przeprowadzenia odbioru:
2. Miejsce przeprowadzenia odbioru:
3. Osoby uczestniczące:
 Przedstawiciele Zamawiającego:

 Przedstawiciele Wykonawcy:

4. Opis sposobu odbioru:
5. Przeprowadzone testy:
6. Rezultaty przeprowadzonych testów:
7. Ujawnione wady lub błędy:
8. Reklamacje zgłoszone przez Zamawiającego:
9. Wnioski dotyczące sposobu usunięcia ujawnionych wad lub błędów, bądź informacja o braku uwag:
- 10, Wykonawca oświadcza, że przekazane kody źródłowe do Nowej wersji Systemu stanowią kompletny kod źródłowy niezbędny do kompilacji Systemu.
.....

Z A M A W I A J Ą C Y:

W Y K O N A W C A:

3. Raport z testowania Nowej wersji Systemu:

Raport z testowania Nowej wersji Systemu:			
RAPORT Z WYKONANIA TESTÓW NR:			
Pełna oraz skrócona nazwa podmiotu, do którego kierowany jest raport:			
Pełna oraz skrócona nazwa systemu			
Umowa nr:		Wersja systemu:	
Pełna oraz skrócona nazwa podmiotu, przeprowadzającego testy:			
Pełna oraz skrócona nazwa oprogramowania testowego:		Wersja oprogramowania testowego:	
Data zakończenia badania:			
Tester (nazwisko, imię, telefon, e-mail osoby przeprowadzającej badanie)			
Lista przeprowadzonych przypadków testowych			
Numer testu (numery testów, począwszy od numeru 1)	Sygnatura przypadku testowego (sygnatury przypadków testowych ze specyfikacji przypadków testowych)	Pozytywny wynik testu (w pozycji należy wpisać znak X, jeżeli wynik testu wypadł pozytywnie)	Negatywny wynik testu (w pozycji należy wpisać znak X, jeżeli wynik testu wypadł negatywnie)
1.			
.....
(numer ostatniego testu)	(sygnatura ostatniego przypadku)		
Lista przeprowadzonych scenariuszy testowych			
Numer testu (numery testów, począwszy od numeru 1)	Sygnatura scenariusza testowego (sygnatury scenariuszy testowych ze specyfikacji scenariuszy testowych)	Pozytywny wynik scenariusza (w pozycji należy wpisać znak X, jeżeli wynik scenariusza wypadł pozytywnie)	Negatywny wynik scenariusza (w pozycji należy wpisać znak X, jeżeli wynik scenariusza wypadł negatywnie)
1.			
.....
(numer ostatniego testu)	(sygnatura ostatniego scenariusza)		
Uwagi do raportu			
Wynik badania (wpisać: TAK lub NIE , co oznacza odpowiednio: poprawne lub niepoprawne wykonanie wszystkich testów i scenariuszy)		Podpis osoby reprezentującej podmiot	

WERYFIKACJA WYKONANYCH TESTÓW NR:	
Pełna oraz skrócona nazwa podmiotu przeprowadzającego weryfikację:	
Pełna oraz skrócona nazwa systemu	

Umowa nr:		Wersja systemu:	
Pełna oraz skrócona nazwa podmiotu, którego oprogramowanie testowe jest poddawane weryfikacji:			
Pełna oraz skrócona nazwa oprogramowania testowego:		Wersja oprogramowania testowego:	
Data zakończenia weryfikacji:			
Przeprowadzający weryfikację <i>(nazwisko, imię, telefon, e-mail pracownika podmiotu przeprowadzającego weryfikację badania)</i>			
Lista zweryfikowanych przypadków testowych			
Numer testu <i>(numery testów, począwszy od numeru 1)</i>	Sygnatura przypadku testowego <i>(sygnatury przypadków testowych ze specyfikacji przypadków testowych)</i>	Pozytywny wynik weryfikacji <i>(w pozycji należy wpisać znak X, jeżeli wynik przypadku wypadł pozytywnie)</i>	Negatywny wynik weryfikacji <i>(w pozycji należy wpisać znak X, jeżeli wynik przypadku wypadł negatywnie)</i>
1.			
.....
<i>(numer ostatniego testu)</i>	<i>(sygnatura ostatniego przypadku)</i>		
Lista zweryfikowanych scenariuszy testowych			
Numer testu <i>(numery testów, począwszy od numeru 1)</i>	Sygnatura scenariusza testowego <i>(sygnatury scenariuszy testowych ze specyfikacji scenariuszy testowych)</i>	Pozytywny wynik weryfikacji <i>(w pozycji należy wpisać znak X, jeżeli wynik scenariusza wypadł pozytywnie)</i>	Negatywny wynik weryfikacji <i>(w pozycji należy wpisać znak X, jeżeli wynik scenariusza wypadł negatywnie)</i>
1.			
.....
<i>(numer ostatniego testu)</i>	<i>(sygnatura ostatniego scenariusza)</i>		
Uwagi do weryfikacji badania			
Wynik weryfikacji <i>(wpisać: TAK lub NIE, co oznacza odpowiednio: poprawne lub niepoprawne wykonanie wszystkich testów i scenariuszy)</i>		Podpis osoby przeprowadzającej weryfikację badania	

4. Wniosek o dostęp do zasobów infrastruktury techniczno-systemowej Ministerstwa Sprawiedliwości (ITS MS)

MINISTERSTWO SPRAWIEDLIWOŚCI <small>www.ms.gov.pl</small>	WNIOSEK	Numer wersji 1.0 Strona 1 z 3
DEPARTAMENT INFORMATYZACJI I REJESTRÓW SĄDOWYCH		
Tytuł: Wniosek o dostęp do zasobów infrastruktury techniczno-systemowej Ministerstwa Sprawiedliwości (ITS MS) - nadanie/modyfikacja/odebranie uprawnień.		
Załącznik nr 1. do Instrukcji "Nadawanie dostępu do zasobów infrastruktury techniczno-systemowej MS (ITS MS)"		
<p><u>PROSZĘ WYPEŁNIAĆ WNIOSEK Z POMOCĄ DOŁĄCZONEJ PONIŻEJ INSTRUKCJI.</u> <u>WNIOSEK WYPEŁNIONY NIEPRAWIDŁOWO / NIEKOMPLETNIE BĘDZIE ODRZUCONY Z PRZYZYNY FORMALNYCH.</u></p>		

Data wpłynięcia wniosku do Sekretariatu DIRS: *wypełnia Sekretariat DIRS											
Imię i nazwisko użytkownika:											
E-mail:						Telefon komórkowy:					
PESEL:											
Nazwa firmy zewnętrznej lub jednostki organizacyjnej Resortu:											
Imię i nazwisko Kierownika projektu po stronie Wykonawcy LUB Przełożonego w przypadku Resortu											
Telefon komórkowy oraz adres e-mail Kierownika projektu po stronie Wykonawcy LUB Przełożonego w przypadku Resortu											
Imię i nazwisko Kierownika projektu /Opiekuna umowy											

po stronie Zamawiającego (MS)									
Wniosek o:	<input type="checkbox"/> nadanie uprawnień	<input type="checkbox"/> modyfikację uprawnień	<input type="checkbox"/> odebranie uprawnień						
Wnioskowana data nadania dostępu:		Data wygaśnięcia dostępu:							
Nazwa Projektu/przedmiot umowy lub uzasadnienie w przypadku odebrania uprawnień:									
Numer umowy:	*pole obowiązkowe tylko w przypadku firmy zewnętrznej								
Data obowiązywania umowy (od - do)	*pole obowiązkowe tylko w przypadku firmy zewnętrznej								
Data obowiązywania usług gwarancyjnych:	*pole obowiązkowe tylko w przypadku firmy zewnętrznej								
System / środowisko:	(np. NKW, KRS, ZSRK, PESEL-SAD etc.)								
Rodzaj/poziom dostępu:	<input type="checkbox"/> środowisko sieciowe	<table border="1"> <tr> <td>SYSTEM OPERACYJNY</td> <td>BAZA DANYCH</td> </tr> <tr> <td><input type="checkbox"/> mainframe</td> <td><input type="checkbox"/> mainframe</td> </tr> <tr> <td><input type="checkbox"/> serwery x86</td> <td><input type="checkbox"/> serwery x86</td> </tr> </table>	SYSTEM OPERACYJNY	BAZA DANYCH	<input type="checkbox"/> mainframe	<input type="checkbox"/> mainframe	<input type="checkbox"/> serwery x86	<input type="checkbox"/> serwery x86	<input type="checkbox"/> obszar aplikacyjny
		SYSTEM OPERACYJNY	BAZA DANYCH						
<input type="checkbox"/> mainframe	<input type="checkbox"/> mainframe								
<input type="checkbox"/> serwery x86	<input type="checkbox"/> serwery x86								
Opis: (np.: TSO, z sieci WAN MS (adresacja IP), z sieci VPN IPSec, z sieci VPN SSL, DB2, x86, etc.)									

Wyszczególnienie zasobów do jakich ma być dostęp:	Opis: (np.: tabele, schematy w bazie danych, porty sieciowe, adresy IP, maszyny wirtualne, etc.)
Oświadczenie Użytkownika*: *wymagane tylko w przypadku wnioskowania o nadanie i modyfikację uprawnień	Oświadczam, że zapoznała(e)m się, rozumiem i będę przestrzegać obowiązków wynikających z: 1. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U z 2014, poz. 1182 j.t.). 2. Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości. 3. Regulaminu Użytkownika Systemów Teleinformatycznych Ministerstwa Sprawiedliwości. i zobowiązuje się do zapewnienia bezpieczeństwa przetwarzania danych poprzez ich ochronę przed udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. regulacji oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także jestem świadom(a) odpowiedzialności jaką ponoszę na podstawie przepisów Regulaminu pracy, Kodeksu Karnego, Kodeksu pracy oraz Ustawy o ochronie danych osobowych. Jednocześnie zobowiązuje się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia do których uzyskam dostęp. Niniejsze oświadczenie potwierdzam własnoręcznym podpisem. <div style="text-align: right;"> _____ Data i podpis oświadczającego </div>

Złożenie zatwierdzenia dla wniosku w procesie zarządzania zmianą za pośrednictwem systemu HP Service Manager (HPSM) jest równoznaczne z odręcznym podpisem. Ten typ zatwierdzenia jest możliwy tylko przy akceptacji oznaczonej jedną gwiazdką *.

Podpisy wymagane w przypadku Wnioskodawcy z Resortu	
<div style="text-align: center;"> _____ Akceptacja** (Przełożony Użytkownika /Kierownik jednostki organizacyjnej resortu /Kierownik projektu) </div> <div style="text-align: center;"> **bezwzględnie wymagany odręczny podpis + pieczętka poprzez system HPSM </div>	<div style="text-align: center;"> _____ Akceptacja DIRS* (Dyrektor DIRS /Naczelnik WUA/WUI) </div> <div style="text-align: center;"> *Możliwość zatwierdzenia </div>
Podpisy wymagane w przypadku Wnioskodawcy z firmy zewnętrznej	
<div style="text-align: center;"> _____ Akceptacja** (Kierownik Projektu Wykonawcy) </div>	<div style="text-align: center;"> _____ Akceptacja* (Kierownik Projektu/Opiekun umowy po stronie Zamawiającego) </div>

****bezwzględnie wymagany odręczny podpis + pieczęćka**

Potwierdzenie realizacji*
(Administrator SPD MS)

Akceptacja DIRS*
(Dyrektor DIRS)

*Możliwość zatwierdzenia poprzez system
HPSM

**5. Załącznik nr 1 do Wniosku o dostęp do zasobów infrastruktury techniczno-systemowej
Ministerstwa Sprawiedliwości (ITS MS)**

MINISTERSTWO SPRAWIEDLIWOŚCI www.ms.gov.pl	Projekt techniczny	Numer wersji 1.0 Strona 1 z 6
DEPARTAMENT INFORMATYZACJI I REJESTRÓW SĄDOWYCH		
Tytuł: Realizacja dostępu do zasobów infrastruktury techniczno-systemowej Ministerstwa Sprawiedliwości		
Załącznik nr 1. do Wniosku o dostęp do zasobów infrastruktury techniczno-systemowej Ministerstwa Sprawiedliwości (ITS MS) – nadanie/modyfikacja/odebranie uprawnień.		

Wnioskujący:

Nazwa firmy ¹ :				
Nazwa projektu/ przedmiot umowy ¹ :				
Nr umowy ¹ :				
Historia zmian w projekcie				
Wersja ²	Data ²	Opis ²	Autor ²	Uwagi ²
1.0	dd-mm-rrrr			

¹ Informacje do uzupełnienia przez firmę zewnętrzną

² Informacje do uzupełnienia przez osobę dokonującą modyfikacji w projekcie

Spis Treści

1. Wprowadzenie	2
2. Topologia logiczna	2
3. Sposób realizacji dostępu	3
4. Ograniczenia dostępu	4
5. Udostępniane zasoby	4
6. Zasady kontroli dostępu i monitorowanie.	5
7. Lista osób upoważnionych	6

Definicje:

VPN – (ang. *Virtual Private Network*, *Wirtualna Sieć Prywatna*) metoda bezpiecznej i prywatnej transmisji danych przez niezabezpieczoną, współdzieloną infrastrukturę sieci (Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Dająca możliwość kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa.

IPSec (IP Security) – zestaw protokołów do zabezpieczenia komunikacji IP zapewniający szyfrowanie, integralność i uwierzytelnianie.

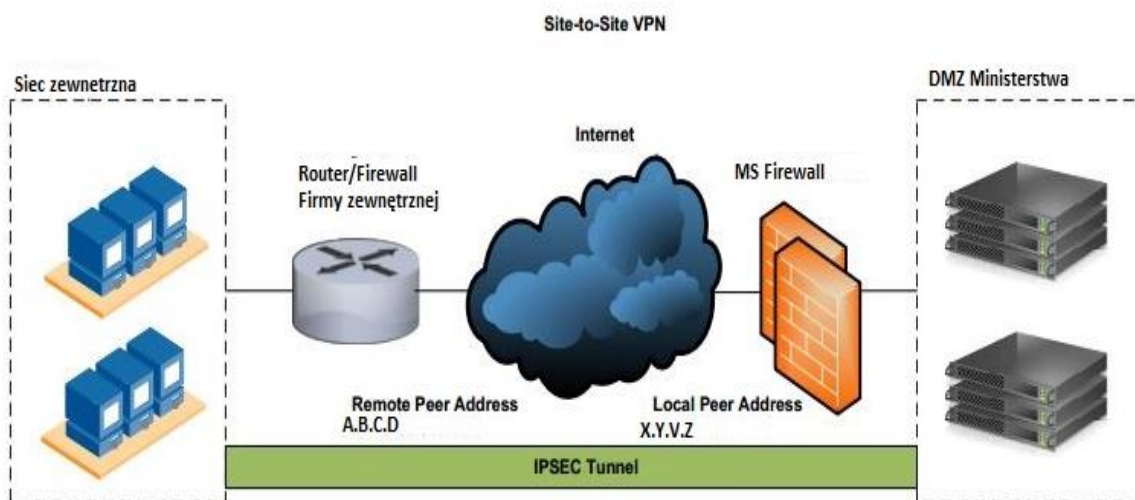
1. Wprowadzenie

Celem dokumentu jest określenie zasad realizacji dostępu do zasobów infrastruktury techniczno-systemowej Ministerstwa Sprawiedliwości. Dostęp ten ma na celu umożliwienie realizacji projektu lub przedmiotu umowy **Wnioskującemu**.

Do zapewnienia bezpiecznego połączenia na potrzeby pracy zdalnej pomiędzy siecią **Wnioskującego**, a siecią Ministerstwa Sprawiedliwości zostanie zestawiony tunel IPSec VPN. Tunel ten zostanie zaszyfrowany z wykorzystaniem możliwie najmocniejszych algorytmów wspieranych przez urządzenia brzegowe **Wnioskującego** i Ministerstwa Sprawiedliwości.

2. Topologia logiczna

Topologia przedstawia informację o sposobie połączenia tunelu IPSec VPN pomiędzy **Wnioskującym** a Ministerstwem Sprawiedliwości



3. Sposób realizacji dostępu

Do zestawienia tunelu IPSec VPN zostaną wykorzystane możliwe najlepsze algorytmy szyfrujące. Dzięki temu zostanie zachowany wysoki poziom bezpieczeństwa danych, które będą przesyłane tunelem VPN. Poniższa tabela zawiera specyfikację techniczną tunelu IPSec VPN wraz z ich opisem.

	Parametr	Wartość	Opis
IKE	Authentication	pre-shared key	Bramki VPN będą uwierzytelniane z użyciem hasła. Hasło zostanie wygenerowane za pomocą generatora losowego i będzie zawierało 12 znaków. Zostanie ono wysłane do administratora za pomocą wiadomości SMS.
	Encryption Algorithm	AES-256	W celu zaszyfrowania tunelu IKE, który posłuży do wymiany informacji przy generowaniu klucza szyfrującego, zostanie wykorzystany najsilniejszy dostępny na urządzeniach algorytm AES-256
	Hash Algorithm	SHA-256	W celu sprawdzenia wiarygodności danych w tunelu IKE zostanie wykorzystana funkcja skrótu SHA-1
	Diffie-Hellman Group	Grupa 5	Do wygenerowania klucza szyfrującego tunel IKE zostanie wykorzystana grupa DH 5, która generuje klucze o długości 1536-bit
	Life Time	28800 sec	Tunel IKE będzie odnawiany co 24 godz. Po każdym odnowieniu tunelu będzie wykorzystywany inny klucz do szyfrowania danych w tunelu IKE.
IPSec	Encryption Algorithm	AES-256	W celu zaszyfrowania tunelu IPSec, który posłuży do przesyłania danych zostanie wykorzystany najsilniejszy dostępny na urządzeniach algorytm AES-256
	Hash Algorithm	SHA-256	W celu sprawdzenia wiarygodności danych w tunelu IPSec zostanie wykorzystana funkcja skrótu SHA-1
	PFS	Tak	Do szyfracji tunelu IPSec zostanie wykorzystany inny klucz niż do szyfracji IKE
	PFS Diffie-Hellman Group	Grupa 5	Do wygenerowania klucza szyfrującego tunel IPSec zostanie wykorzystana grupa DH 5, która generuje klucze o długości 1536-bit
	Life Time	3600sec	Tunel IPSec będzie odnawiany co 1 godz. Po każdym odnowieniu tunelu będzie wykorzystywany inny klucz do szyfracji danych w tunelu IPSec

4. Ograniczenia dostępu

Dostęp za pomocą tunelu IPSec VPN zostanie ograniczony tylko dla określonych osób, wskazanych przez **Wnioskującego**. W tym celu w sieci **Wnioskującego** zostanie stworzona nowa podsieć: 10.60.X.0/24 zaproponowana przez „Zespół sieci” MS. Tylko ta podsieć zostanie przepuszczona przez tunel VPN.

W tabeli poniżej zawarte są podsieci IP, do których zostanie zapewniony dostęp za pomocą tunelu VPN oraz informacja pomiędzy jakimi urządzeniami zostanie zestawiony tunel VPN.

Remote network ³	Remote Peer Address ¹	Local Peer Address ³	MS DMZ network ³

Nazwa urządzenia ¹	Model ¹	Wersja oprogramowania ¹

¹ Informacje do uzupełnienia przez firmę zewnętrzną

³ Informacje do uzupełnienia przez „Zespół sieci” MS

5. Udostępniane zasoby

Poniższa tabela zawiera spis adresów IP oraz numerów portów, które są niezbędne do zapewnienia odpowiedniego dostępu do aplikacji w realizowanym projekcie przez **Wnioskującego**.

Dzięki przepuszczeniu tych adresów przez tunel IPsec VPN będzie możliwa praca pracowników z siedziby firmy **Wnioskującego** na poziomie porównywalnym jak po połączeniu z sieci LAN Ministerstwa Sprawiedliwości.

W tabeli umieszczono informacje, do których zasobów powinni mieć dostęp pracownicy firmy

Wnioskującego

Serwery:

LP	Adres IP ⁴	Hostname ⁴	Środowisko ⁴	Porty TCP/UDP/ICMP ⁴
1.				
2.				
3.				

Bazy Danych:

LP	Adres IP ⁴	Instancja/Region/ Nazwa bazy danych ⁴	Środowisko silnika bazodanowego ⁴	Uprawnienia [Select, Insert, Update, Delete] ⁴	Porty CP/UDP/ICMP ⁴
1.					
2.					
3.					

Aplikacje:

LP	Nazwa aplikacji/SID ⁴	Adres do aplikacji- Ścieżka http (s) ⁴	Porty TCP/UDP/ICMP ⁴
1.			
2.			
3.			

⁴Informacje do uzupełnienia przez Administratora z MS

6. Zasady kontroli dostępu i monitorowanie.

Wnioskujący przekaże listę uprawnionych użytkowników z określonym terminem ważności konta, celem dostępu w postaci „karty dostępu”. Pracownicy Ministerstwa Sprawiedliwości wygenerują konta użytkowników, loginy i hasła zostaną przekazane wraz z instrukcją logowania **Wnioskującemu**.

W celu uzyskania dostępu do zasobów Ministerstwa Sprawiedliwości każdy użytkownik będzie podlegał weryfikacji w procesie uwierzytelnienia. Na urządzeniu terminującym zostanie skonfigurowany mechanizm „Captive Portal”, zapewniający dostęp tylko autoryzowanym użytkownikom. W przypadku wprowadzenia niepoprawnego hasła trzykrotnie konto użytkownika zostanie zablokowane. Po poprawnym zalogowaniu użytkownik otrzyma dostęp do wskazanych zasobów, a jego ruch będzie monitorowany.

Do rejestracji połączeń użytkowników łączących się za pomocą tunelu VPN do sieci Ministerstwa Sprawiedliwości na urządzeniu **Wnioskującego** zostanie włączone logowanie ruchu przechodzącego przez tunel IPsec. Dzięki temu będzie istniała możliwość przygotowania przez **Wnioskującego** raportu zawierającego informację jaki użytkownik w jakim czasie i do jakich zasobów się łączył. Raport będzie przekazywany do Ministerstwa Sprawiedliwości w każdym pierwszym roboczym tygodniu miesiąca za miesiąc poprzedni.

7. Lista osób upoważnionych

W przypadku zmiany osób upoważnionych do dostępu lub zmiany pozostałych danych w poniższej tabeli **Wnioskujący** przekaże do Ministerstwa Sprawiedliwości uaktualnioną wersję niniejszego dokumentu.

L.p	Imię i Nazwisko ¹	Data rozpoczęcia ¹	Data zakończenia ¹	E-mail ¹	Telefon komórkowy ¹
1.					
2.					
3.					
4.					
5.					

¹Informacje do uzupełnienia przez firmę zewnętrzną

<p>-----</p> <p>Akceptacja Kierownika Projektu ze strony Wnioskującego ¹ (podpis odręczny i pieczęć imienna)</p>	<p>-----</p> <p>Akceptacja Kierownika Projektu/opiek Umowy ze strony MS (podpis odręczny/akceptacja udzi elektronicznie w procesie zarząd zmianą za pośrednictwem system HPSM)</p>
<p>-----</p> <p>Potwierdzenie realizacji przez Administratora SPD MS (podpis odręczny/akceptacja udzielona elektronicznie w procesie zarządzania zmianą za pośrednictwem systemu HPSM)</p>	<p>-----</p> <p>Akceptacja Dyrektora DIRS (podpis odręczny/akceptacja udzi elektronicznie w procesie zarządza zmianą za pośrednictwem systemu H</p>

6. Protokół odbioru Dokumentacji Systemu:

Protokół odbioru Dokumentacji Systemu			
-----		-----	
Wypełnia			
Wykonawca/Zamawiają			
cy			
Formularz odbioru Dokumentacji		Nr Zgłoszenia:	
		Data:	- -
		Godzina:	.
		Rodzaj błędu:	
		Serwis gwarancyjny	
		(T/N):	
Departament Informatyzacji i Rejestrów Sądowych/.....			
Imię i			
nazwisko:			
		System:	
		Wersja:	
Opis szczegółowy:			
W załączeniu:			
ZAMAWIAJĄCY/WYKONAWCA			
-----		-----	
Wypełnia			
Wykonawca/Zamawiający			
<nazwa firmy>			
Imię i		Data:	- -
nazwisko:		Godzina:	.

przyjmuje Dokumentację:

1.

2.

...

Działania proponowane:



WYKONAWCA/ZAMAWIAJĄCY

Wypełnia

Wykonawca/Zamawiający

Adnotacje dot. Dokumentacji

