

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

Załącznik nr 6 do Zasad Zarządzania Bezpieczeństwem Informacji

(Załącznik nr ... do Umowy/Porozumienia nr z dnia ...)*

Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego

Dokument wydrukowany i niepodpisany jest dokumentem nienadzorowanym.

Opracowali:	Sprawdzili:	Zatwierdzili:
Inspektor Ochrony Danych w SA we Wrocławiu Katarzyna Sandecka Główny Specjalista ds. Bezpieczeństwa IT w Oddziale Informatycznym SA we Wrocławiu Przemysław Szymanek Główny Administrator Bezpieczeństwa Informacji SA we Wrocławiu Dariusz Kania	Kierownik Oddziału Informatycznego w Sądzie Apelacyjnym we Wrocławiu Krzysztof Kamiński	Prezes Sądu Apelacyjnego we Wrocławiu Jacek Gołaczyński (podpisano elektronicznie) Dyrektor Sądu Apelacyjnego we Wrocławiu Artur Moneta (podpisano elektronicznie)

Pełny zakres dostępu do dokumentu – odczyt, modyfikacja, usuwanie, dodawanie:

1. Prezes Sądu Apelacyjnego we Wrocławiu;
2. Dyrektor Sądu Apelacyjnego we Wrocławiu;
3. Główny Administrator Bezpieczeństwa Informacji;
4. Główny specjalista ds. bezpieczeństwa IT;
5. Inspektor Ochrony Danych;
6. Administrator Bezpieczeństwa Systemu Informatycznego.

Zakres dostępu do dokumentu – odczyt:

7. Podmioty Zewnętrzne realizujące zadania w Systemie Informatycznym Sądu Apelacyjnego we Wrocławiu;
8. Osoby uzyskujące dostęp zdalny do zasobów sieciowych innych jednostek Resortu za pośrednictwem łącza VPN Sądu Apelacyjnego we Wrocławiu;
9. Pracownicy Oddziału Informatycznego;
10. Pozostali pracownicy odpowiedzialni za realizację umów lub porozumień z Podmiotami Zewnętrznymi ze strony Sądu Apelacyjnego we Wrocławiu;
11. Kierownicy Komórek Organizacyjnych;
12. Podmioty i instytucje upoważnione na podstawie przepisów prawa.

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

* niepotrzebne skreślić

KARTA ZMIAN:			
Nr	Opis dokonanej zmiany w treści dokumentu	Data zmiany	Podpis uprawnionego pracownika
1	Zaktualizowano dokument, zgodnie z ZARZĄDZENIEM nr 0212-9/20 Prezesa Sądu Apelacyjnego we Wrocławiu i Dyrektora Sądu Apelacyjnego we Wrocławiu z dnia 8 maja 2020 r. w sprawie powołania Zespołu do realizacji przeglądu okresowego Systemu Zarządzania Bezpieczeństwem Informacji w Sądzie Apelacyjnym we Wrocławiu.	29.05.2020 r.	Zespół powołany na podstawie ww. zarządzenia
2	Zaktualizowano dokument, zgodnie z Zarządzeniem nr 0212-2/22 Prezesa Sądu Apelacyjnego we Wrocławiu i Dyrektora Sądu Apelacyjnego we Wrocławiu z dnia 3 lutego 2022 r. w sprawie powołania Zespołu do realizacji przeglądu okresowego Systemu Zarządzania Bezpieczeństwem Informacji w Sądzie Apelacyjnym we Wrocławiu.	19.08.2022 r.	Zespół powołany na podstawie ww. zarządzenia
3	Dokonano przeglądu dokumentu zgodnie z Zarządzeniem nr 0212-19/23 Prezesa Sądu Apelacyjnego we Wrocławiu i Dyrektora Sądu Apelacyjnego we Wrocławiu z dnia 16 listopada 2023 r. w sprawie powołania Zespołu do realizacji przeglądu okresowego Systemu Zarządzania Bezpieczeństwem Informacji w Sądzie Apelacyjnym we Wrocławiu.		Zespół powołany na podstawie ww. zarządzenia
4	Zaktualizowano dokument zgodnie z Zarządzeniem nr 023.20.2024 Prezesa Sądu Apelacyjnego we Wrocławiu i Dyrektora Sądu Apelacyjnego we Wrocławiu z dnia 18 grudnia 2024 r. w sprawie powołania Zespołu do realizacji przeglądu okresowego Systemu Zarządzania Bezpieczeństwem Informacji w Sądzie Apelacyjnym we Wrocławiu oraz Zespołu do wypracowania jednolitych standardów i procedur bezpieczeństwa informacji z zakresu obsługi informatycznej sądów okręgowych i rejonowych z obszaru apelacji wrocławskiej.		Zespół powołany na podstawie ww. zarządzenia
5			
6			
7			
8			
9			
10			

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

Spis treści

Spis treści.....	3
§ 1 Cel.....	4
§ 2 Zakres	4
§ 3 Słownik	5
§ 4 Postanowienia ogólne	5
§ 5 Nadawanie, zmiana bądź odebranie uprawnień w Systemie Informatycznym Sądu dla Wykonawców	5
§ 6 Nadawanie, zmiana bądź odebranie uprawnień w Systemie Informatycznym Sądu dla pracowników innych Jednostek Resortu.....	7
§ 7 Metody i środki uwierzytelniania	9
§ 8 Hasła	9
§ 9 Konta administracyjne.....	10
§ 10 Dostęp zdalny do systemów informatycznych Sądu	11
§ 11 Zasady dostępu zdalnego dla Wykonawców lub pracowników innych Jednostek Resortu, którzy uzyskują dostęp do zasobów sieciowych tych Jednostek za pośrednictwem łącza VPN Sądu	12
§ 12 Wymagania zabezpieczeń	13
§ 13 Reagowanie na incydenty	14
§ 14 Odpowiedzialność	15
§ 15 Postanowienia końcowe	15
§ 16 Lista dokumentów związanych	16
§ 17 Załączniki	16

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

§ 1 Cel

1. Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego Sądu Apelacyjnego we Wrocławiu, zwany dalej Regulaminem określa:
 - 1) minimalne wymagania bezpieczeństwa informacji dla:
 - a) Wykonawców świadczących usługi na rzecz Sądu Apelacyjnego we Wrocławiu (zwanego dalej: Sądem) na podstawie łączących Strony umów i porozumień (zwanych dalej: „umową” lub „umowami”) oraz
 - b) pracowników innych Jednostek Resortu (rozumiane jako jednostki resortu podległe lub nadzorowane przez Ministra Sprawiedliwości zwane dalej: „inne Jednostki Resortu”), którzy wykonują prace w Systemie Informatycznym Sądu (ilekroć w niniejszym Regulaminie jest mowa o Systemie Informatycznym Sądu, należy przez to rozumieć również Sądowe Systemy Teleinformatyczne, dla których powierzono Sądowi czynności związane z ich projektowaniem, wdrożeniem i utrzymaniem na podstawie odpowiednich przepisów prawa) na podstawie powierzonych obowiązków,
 - c) Wykonawców i pracowników innych Jednostek Resortu, którzy uzyskują dostęp zdalny do zasobów sieciowych innych Jednostek Resortu za pośrednictwem łącza VPN Sądu,

które dla potrzeby niniejszego Regulaminu określa się dalej łącznie Podmiotami Zewnętrznymi;
 - 2) minimalne wymagania zabezpieczeń Systemu Informatycznego Sądu;
 - 3) zasady nadawania i odbierania dostępu zdalnego do zasobów sieciowych tych Jednostek Resortu za pośrednictwem łącza VPN Sądu;
 - 4) zakres obowiązków i odpowiedzialności ww. podmiotów w odniesieniu do bezpieczeństwa informacji.

§ 2 Zakres

1. Niniejszy Regulamin:
 - 1) ma zastosowanie do wszystkich umów zawartych z Wykonawcami, których przedmiot jest związany z przetwarzaniem aktywów informacyjnych Sądu i wynikającą stąd potrzebą ochrony informacji;
 - 2) stosują:
 - a) wszystkie Podmioty Zewnętrzne realizujące prace na rzecz Sądu, związane z przetwarzaniem aktywów informacyjnych Sądu;
 - b) wszystkie Podmioty Zewnętrzne realizujące czynności w Sądowych Systemach Teleinformatycznych na podstawie umów zawartych z Sądem lub odpowiednich przepisów odrębnych oraz
 - c) Podmioty Zewnętrzne uzyskujące dostęp zdalny do zasobów sieciowych Sądu i innych Jednostek Resortu za pośrednictwem łącza VPN Sądu.
2. Regulamin obejmuje swym zakresem wszystkich pracowników Podmiotów Zewnętrznych, mających dostęp do Systemu Informatycznego Sądu lub uzyskujących dostęp zdalny do zasobów sieciowych innych Jednostek

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

Resortu za pośrednictwem łącza VPN Sądu. Na potrzeby niniejszego Regulaminu przez pracowników Podmiotu Zewnętrznego rozumiemy również jego podwykonawców i osoby wykonujące czynności na podstawie innego rodzaju umów cywilnoprawnych.

- Regulamin w sposób syntetyczny opisuje zasady zawarte w dokumentach Systemu Zarządzania Bezpieczeństwem Informacji, w szczególności w Polityce Bezpieczeństwa Informacji, Polityce Bezpieczeństwa Systemu Informatycznego, Polityce Ochrony Danych Osobowych Sądu.

§ 3 Słownik

Pozostałe pojęcia używane w niniejszym Regulaminie, a w nim niewyjaśnione, zdefiniowane zostały w ***Słowniku pojęć używanych w dokumentach Systemu Zarządzania Bezpieczeństwem Informacji Sądu***.

§ 4 Postanowienia ogólne

- Podmiot Zewnętrzny musi spełniać wymagania niniejszego Regulaminu przed uzyskaniem dostępu do zasobów informacyjnych Sądu (w tym Systemu Informatycznego oraz aktywów informacyjnych Sądu przetwarzanych w innej postaci) albo przed uzyskaniem dostępu zdalnego do zasobów sieciowych innych Jednostek Resortu za pośrednictwem łącza VPN Sądu.
- Jeżeli realizacja umowy przez Podmiot Zewnętrzny związana jest z przetwarzaniem danych osobowych, których administratorem lub podmiotem przetwarzającym jest odpowiednio Sąd, Prezes lub Dyrektor Sądu (w zakresie realizowanych przez te podmioty zadań), Wykonawca przed przystąpieniem do ich przetwarzania powinien spełnić poniższe warunki:
 - zobowiązany jest uprawdopodobnić, że spełnia wymagania przewidziane w art. 28 ust. 1 i 2 oraz ust. 4 RODO dla podmiotu przetwarzającego oraz
 - wdraża i stosuje odpowiednie środki techniczne i organizacyjne, o których mowa w art. 32 ust. 1 w zw. z ust. 2 RODO lub odpowiednio w art. 34 ust. 2 i ust. 5 uODO i jest w stanie to wykazać, np. poprzez wypełnienie listy kontrolnej, która stanowi załącznik do umowy powierzenia przetwarzania danych osobowych;
 - zawrzeć umowę powierzenia przetwarzania danych osobowych, w szczególności na wzorze obowiązującym w Sądzie, zgodnie z Polityką Bezpieczeństwa Danych Osobowych Sądu.

§ 5 Nadawanie, zmiana bądź odebranie uprawnień w Systemie Informatycznym Sądu dla Wykonawców

- O ile zasady nadawania, zmiany bądź odebrania uprawnień nie są odrębnie uregulowane w dokumentacji bezpieczeństwa usługi lub systemu, należy stosować poniższe zasady.
- Wykonawca, mający świadczyć usługi związane z pracą w Systemie Informatycznym Sądu, przed rozpoczęciem realizacji tych prac, powinien zapoznać się z niniejszym Regulaminem i stosować jego zasady. Wykonawca odpowiada jednocześnie za zapoznanie z niniejszym Regulaminem członków personelu, którym się posługuje przy realizacji umowy, i egzekwowanie jego zapisów.
- Zakres uprawnień w poszczególnych systemach i usługach Sąd przydziela adekwatnie do przedmiotu zawartej umowy, do zakresu powierzonych do przetwarzania danych osobowych albo zakresu powierzonych czynności.

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

4. Osoba odpowiedzialna za realizację umowy po stronie Wykonawcy zobowiązana jest dostarczyć listę personelu, którym będzie się posługiwać przy realizacji umowy, o ile to możliwe na 5 dni roboczych (przez dzień roboczy należy rozumieć dzień od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy oraz dni uznanych za wolne od pracy w Sądzie) przed rozpoczęciem pracy w Systemie Informatycznym Sądu. Wzór listy stanowi Załącznik nr 3 do niniejszego Regulaminu.
5. W przypadku personelu Wykonawcy, któremu ma być założone konto w celu zapewnienia dostępu do Systemu Informatycznego:
 - 1) lista, o której mowa powyżej, powinna zawierać:
 - a) login AD (jeżeli użytkownik go posiada),
 - b) indywidualny adres poczty elektronicznej dla każdego członka personelu Wykonawcy (tzw. służbowy adres poczty elektronicznej),
 - c) a w przypadku nadania dostępu za pośrednictwem łącza VPN dla Wykonawców – również numer telefonu komórkowego tej osoby, na który zostaną wysłane informacje niezbędne do zalogowania.
 - 2) W niektórych przypadkach, wymuszonych funkcjonalnością systemu wymagane będzie dodatkowo wskazanie numeru PESEL osoby, dla której ma być ten dostęp nadany; numer PESEL może zostać przekazany wraz z listą osób lub oddzielnie, z zachowaniem zasad bezpieczeństwa i poufności, np. w pliku zabezpieczonym hasłem.
 - 3) osoba odpowiedzialna za realizację umowy po stronie Sądu z wyprzedzeniem poinformuje Wykonawcę o potrzebie wskazania numerów PESEL i wyjaśni cel i zakres przetwarzania tych danych.
6. Po każdej zmianie personelu, jeżeli umowa łącząca strony nie stanowi inaczej, Wykonawca zobowiązany jest niezwłocznie, jednak nie później, niż w terminie 5 dni roboczych od dokonania zmiany, do zgłoszenia zmian lub przekazania aktualnej listy personelu ze wskazaniem zmian w zakresie ich uprawnień.
7. Wykonawca zobligowany jest do monitorowania realizacji prac przez wskazane osoby oraz odpowiada za działania mające na celu niezwłoczne odebranie uprawnień do Systemu Informatycznego Sądu osobom, które nie wykonują już czynności na rzecz Sądu.
8. Rejestrowanie/wyrejestrowanie personelu Wykonawcy w Systemie Informatycznym Sądu oraz nadawanie/zmiana/odebranie uprawnień jest realizowane przez Sąd zgodnie ze schematem postępowania:
 - 1) Wykonawca przekazuje listę personelu w sposób bezpieczny (w szczególności w zaszyfrowanym pliku, do którego hasło przekazywane jest innym kanałem komunikacji), wraz z podpisanym przez każdą z tych osób oświadczeniem stanowiącym Załącznik nr 1 do niniejszego Regulaminu do osoby odpowiedzialnej za realizację umowy po stronie Sądu. Lista osób, o ile zawiera numery PESEL, może być przechowywana po zanonimizowaniu numerów PESEL lub usunięta przez Przedstawiciela Sądu po pomyślnym założeniu kont w Systemie Informatycznym.
 - 2) Przedstawiciel Sądu wnioskuje o nadanie/zmianę/odebranie uprawnień dla personelu Wykonawcy. W razie

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

wątpliwości uzyskuje akceptację wniosku przez Kierownika Komórki Organizacyjnej lub Dyrektora Sądu.

- 3) Podczas rejestracji ww. osób w Systemie Informatycznym Sądu nadawany jest unikalny identyfikator oraz ustawiane jest unikalne hasło tymczasowe niezbędne do pierwszego logowania do Systemu Informatycznego Sądu.
- 4) Przedstawiciel Sądu lub Administrator Systemu informuje o nadaniu uprawnień Wykonawcę. Administrator Systemu odpowiada ze przekazanie danych uwierzytelniających indywidualnie poszczególnym członkom personelu Wykonawcy.
- 5) Administrator Systemu przekazuje dane uwierzytelniające indywidulanie w sposób bezpieczny:
 - a) identyfikator (login) lub link niezbędny do pierwszego logowania przesyłany jest za pomocą poczty e-mail;
 - b) jeżeli przekazany został numer telefonu komórkowego członka personelu, Administrator Systemu przesyła hasło pierwszego logowania poprzez wiadomość SMS;
 - c) w wyjątkowych sytuacjach, gdy nie został przekazany numeru telefonu komórkowego, dopuszcza się przekazanie hasła i loginu przy użyciu różnych kanałów komunikacyjnych, w szczególności:
 - w trakcie rozmowy telefonicznej, po upewnieniu się, że rozmówcą jest uprawniony członek personelu Wykonawcy;
 - poprzez wiadomość e-mail;
 - osobiście;
 - z wykorzystaniem operatora pocztowego;
 - w inny bezpieczny sposób ustalony z Wykonawcą.
- 6) Hasło przekazywane za pomocą metod wskazanych w pkt 5) lit. c tiret drugie powinno być zabezpieczone za pomocą jednej z poniższych metod:
 - a) przesłanie w wiadomości e-mail maksymalnie połowy znaków hasła, a pozostała część jest przekazywana za pomocą innego kanału komunikacyjnego np. w trakcie rozmowy telefonicznej;
 - b) zaszyfrowanie hasła w wiadomości e-mail, po ustaleniu z Wykonawcą lub członkiem personelu klucza deszyfrującego.
9. Zobowiązuje się Wykonawcę, który przekazuje dane członków personelu do przekazania im klauzul informacyjnych dotyczących Sądu - spełnienie obowiązku informacyjnego przewidzianego odpowiednio w art. 13 i 14 RODO. Klauzule informacyjne Sądu dostępne są m.in. na stronie podmiotowej BIP Sądu, w zakładce: RODO.

§ 6 Nadawanie, zmiana bądź odebranie uprawnień w Systemie Informatycznym Sądu dla pracowników innych Jednostek Resortu

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

1. O ile zasady nadawania, zmiany bądź odebrania uprawnień nie są odrębnie uregulowane w dokumentacji bezpieczeństwa usługi lub systemu, należy stosować poniższe zasady.
2. Pracownicy innych Jednostek Resortu, mający świadczyć usługi związane z pracą w Systemie Informatycznym Sądu (w tym w centralnych sądowych systemach teleinformatycznych utrzymywanych przez Sąd), przed rozpoczęciem realizacji tych prac, powinni zapoznać się z dokumentacją bezpieczeństwa tych systemów i niniejszym Regulaminem.
3. Zakres uprawnień w poszczególnych systemach i usługach przydziela się adekwatnie do zakresu powierzonych czynności i obowiązków służbowych.
4. Rejestrowanie/wyrejestrowanie użytkowników w Systemie Informatycznym Sądu oraz nadawanie/zmiana/odebranie uprawnień jest realizowane przez Sąd zgodnie ze schematem postępowania:
 - 1) Kierownik innej Jednostki Resortu zobowiązany jest dostarczyć listę pracowników, o ile to możliwe na 5 dni roboczych (przez dzień roboczy należy rozumieć dzień od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy oraz dni uznanych za wolne od pracy w Sądzie) przed rozpoczęciem pracy w Systemie Informatycznym Sądu. Wzór listy stanowi Załącznik nr 3 do niniejszego Regulaminu.
 - 2) Listę przekazuje się w sposób bezpieczny, wraz z podpisanym przez każdą z tych osób oświadczeniem stanowiącym Załącznik nr 2 do niniejszego Regulaminu do osoby odpowiedzialnej za realizację przez Sąd czynności powierzonych na podstawie odpowiednich aktów prawnych (zwaną dalej: Przedstawiciel Sądu).
 - 3) W przypadku potrzeby nadania dostępu zdalnego, do listy powinny również zostać dołączone podpisane przez każdego pracownika oświadczenia stanowiące Załącznik nr 1 do niniejszego Regulaminu.
 - 4) Przedstawiciel Sądu wnioskuje o nadanie/zmianę/odebranie uprawnień. W razie wątpliwości uzyskuje akceptację wniosku przez Kierownika Komórki Organizacyjnej lub Dyrektora Sądu.
 - 5) Przed nadaniem dostępu do centralnych sądowych systemach teleinformatycznych, wymagane jest nadanie pracownikom upoważnienia do przetwarzania danych osobowych. Upoważnienie to powinno być nadane przez inną Jednostkę Resortu wnioskującą o dostęp do systemu. Upoważnienie może przyjąć również postać elektroniczną.
 - 6) Podczas rejestracji ww. osób w Systemie Informatycznym Sądu nadawany jest unikalny identyfikator oraz ustawiane jest unikalne hasło tymczasowe niezbędne do pierwszego logowania do Systemu Informatycznego Sądu.
 - 7) Przedstawiciel Sądu lub Administrator Systemu informuje o nadaniu uprawnień pracowników. Administrator Systemu odpowiada ze przekazanie danych uwierzytelniających indywidualnie poszczególnym pracownikom.
 - 8) Administrator Systemu przekazuje dane uwierzytelniające indywidulanie każdemu pracownikowi w sposób

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

bezpieczny na zasadach określonych w § 5 ust. 5 i 6.

- 9) Kierownik innej Jednostki Resortu, który przekazuje dane swoich pracowników zobowiązany jest do spełnienia obowiązku informacyjnego przewidzianego w art. 13 i 14 RODO, również w imieniu Sądu Apelacyjnego we Wrocławiu.

5. Lista, o której mowa powyżej, powinna zawierać login AD i służbowy adres poczty elektronicznej tych osób.

§ 7 Metody i środki uwierzytelniania

Dostęp do poszczególnych składników Systemu Informatycznego Sądu jest możliwy wyłącznie poprzez podanie prawidłowego identyfikatora i hasła przyznanych pracownikowi podczas procesu nadawania uprawnień do Systemu Informatycznego Sądu.

§ 8 Hasła

1. Hasła do Systemu Informatycznego Sądu powinny podlegać następującym zasadom:
 - 1) hasło administracyjne składa się z minimum 14 znaków, musi być zmieniane minimum raz w roku,
 - 2) hasło do konta zwykłego składa się z minimum 12 znaków, rekomendowana jest długość hasła nie mniejsza niż 15 znaków; musi być zmieniane minimum co 90 dni,
 - 3) dla kont technicznych zasady haseł ustalane są niezależnie i indywidualnie dla każdego z Systemów Informatycznych Sądu,
 - 4) hasło musi spełniać warunek złożoności polegający na występowaniu w hasle administracyjnym: wielkiej i małej litery, dwóch cyfr i znaku specjalnego (np. !@#).
 - 5) Występowaniu w hasle zwykłym: wielkiej i małej litery oraz cyfry i znaku specjalnego (np. !@#),
 - 6) kolejne hasła muszą być różne,
 - 7) hasła należy przechowywać w sposób gwarantujący ich poufność.
2. Zabrania się udostępniania haseł innym osobom.
3. Zabrania się tworzenia haseł na podstawie:
 - 1) cech i numerów osobistych (np. numerów PESEL, dat urodzenia, numerów telefonów, imion itp.),
 - 2) informacji powszechnie dostępnych na temat pracownika np. w portalach społecznościowych, bieżących dat, tj.: miesiąc i rok, itp.;
 - 3) sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

4) identyfikatora pracownika.

4. W przypadku logowania do Systemu Informatycznego Sądu odbywającego się po raz pierwszy, pracownik Podmiotu Zewnętrznego ma obowiązek zmiany hasła tymczasowego na właściwe, znane tylko temu pracownikowi (jeśli System Informatyczny Sądu umożliwia taką zmianę).
5. W przypadku Systemu Informatycznego Sądu, który nie wymusza automatycznie cyklicznej zmiany hasła oraz nie kontroluje jego złożoności, obowiązkiem każdego użytkownika tego systemu jest zmiana hasła zgodnie z zasadami określonymi w poprzednich ustępach.
6. Pracownik Podmiotu Zewnętrznego ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.
7. Hasła nie mogą być ujawniane w sposób celowy lub przypadkowy i powinny być znane wyłącznie pracownikowi.
8. Pracownik utrzymuje w tajemnicy hasła umożliwiające dostęp do Systemu Informatycznego Sądu również po upływie ich ważności.
9. Hasła nie powinny być przekazywane ani przesyłane przez pracownika za pomocą faksu ani poczty e-mail w formie jawnej.
10. Hasła nie powinny być przechowywane w formie dostępnej dla osób nieupoważnionych:
 - 1) w plikach,
 - 2) na kartkach papieru w miejscach dostępnych dla osób trzecich,
 - 3) w skryptach,
 - 4) w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.
11. W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, hasła muszą być natychmiast zmienione przez pracownika Podmiotu Zewnętrznego, a zdarzenie niezwłocznie zgłoszone Przedstawicielowi Sądu.

§ 9 Konta administracyjne

1. W przypadku świadczenia usługi polegającej na udostępnieniu lub instalacji nowego urządzenia (np. serwera) lub aplikacji przez Podmiot Zewnętrzny, jego przedstawiciel przekazuje dane do konta administracyjnego z najwyższymi uprawnieniami Przedstawicielowi Sądu lub innej osobie wskazanej przez Kierownika Oddziału Informatycznego.
2. W przypadku określonym w ust. 1 Podmiot Zewnętrzny zobowiązany jest również do przekazania Sądowi, na żądanie Przedstawiciela Sądu, procedury aktualizacji oprogramowania zainstalowanego na ww. urządzeniach.
3. Podmiot Zewnętrzny, w przypadku, gdy jest to podyktowane zakresem zawartej z Sądem umowy oraz możliwościami technicznymi Sądu, uzyskuje dostęp administracyjny do Systemu Informatycznego Sądu przy użyciu systemu dedykowanego do zarządzania hasłami w Sądzie.
4. Sesje Podmiotu Zewnętrznego w Systemie Informatycznym Sądu w celu zapewnienia ochrony aktywów informacyjnych i bezpieczeństwa informacji mogą być monitorowane za pomocą rozwiązań służących do monitorowania dostępu uprzywilejowanego.

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

§ 10 Dostęp zdalny do systemów informatycznych Sądu

1. Dostęp zdalny Podmiotu Zewnętrznego możliwy jest tylko po spełnieniu warunków wymienionych w niniejszym Regulaminie.
2. Pracownicy innych Jednostek Resortu mający otrzymać dostęp zdalny do Systemu Informatycznego Sądu muszą być przeszkoleni przez te Jednostki Resortu z przepisów dot. ochrony danych osobowych i bezpieczeństwa informacji.
3. Dostęp do Systemu Informatycznego Sądu może uzyskać tylko personel Wykonawcy przeszkolony z przepisów dot. ochrony danych osobowych i zapoznany z niniejszym Regulaminem.
4. Administrator Bezpieczeństwa Systemu Informatycznego Sądu (dalej również: ABSI) lub osoba przez niego wskazana prowadzi wykaz osób posiadających dostęp zdalny do Systemu Informatycznego Sądu lub uzyskujących dostęp zdalny do zasobów sieciowych za pośrednictwem łącza VPN Sądu.
5. Sąd udziela dostępu zdalnego personelowi Wykonawcy na czas obowiązywania umowy lub realizacji określonego zadania wynikającego z przedmiotu umowy, jednak nie dłużej niż 12 miesięcy, zaś pracownikom innych Jednostek Resortu udziela na czas realizacji zadań. Dostęp zdalny może zostać przedłużony na wniosek Przedstawiciela Sądu, po potwierdzeniu przez Podmiot Zewnętrzny, że lista osób zgłoszonych do realizacji prac jest aktualna.
6. Podmiot Zewnętrzny jest zobowiązany do poinformowania o potrzebie odebrania dostępu zdalnego.
7. Wykonawca, przed przystąpieniem do prac polegających na modyfikacji Systemu Informatycznego Sądu, ustala z Przedstawicielem Sądu scenariusz planowanych prac oraz informuje o identyfikowanych ryzykach, w tym dla bezpieczeństwa informacji.
8. W ramach uzyskanego dostępu zabrania się Podmiotowi Zewnętrznemu przeprowadzać jakichkolwiek operacji mogących prowadzić do nieuzgodnionej utraty lub uszkodzenia danych.
9. Podmiot Zewnętrzny przystępując do czynności, które identyfikuje się jako zagrożone wysokim ryzykiem naruszenia bezpieczeństwa Systemu Informatycznego Sądu lub utraty danych, musi poinformować o takim ryzyku Przedstawiciela Sądu. Czynności mogą być kontynuowane wyłącznie po pisemnej (również w postaci wiadomości elektronicznej) akceptacji tych czynności przez Przedstawiciela Sądu lub ABSI.
10. Wykonywanie prac polegających na:
 - a) obsłudze serwisowej niezwiązanej z wysokimi ryzykami dla bezpieczeństwa Systemu Informatycznego Sądu,
 - b) pracach w środowisku testowym nad rozwojem programu/usługi/systemu będącego w fazie wdrażania,
 - c) pracach lub usługach wykonywanych ciągle, niezwiązanych z wysokimi ryzykami dla bezpieczeństwa Systemu Informatycznego Sądu (np. utrzymanie lub monitoring Systemu Informatycznego Sądu)
 nie wymaga każdorazowego ustalenia warunków realizacji tych prac. W ramach wykonywania tych prac obowiązują warunki uzgadniane na bieżąco pomiędzy Przedstawicielami Sądu i Wykonawcy.
11. Przedstawiciel Sądu we współpracy z wyznaczonym Administratorem Systemu ogranicza zasoby dostępne dla sesji zdalnej do niezbędnego minimum, przy zachowaniu poniższych reguł:

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

- 1) Administrator Systemu tworzy listę zasobów dostępnych dla sesji zdalnej Podmiotu Zewnętrznego;
 - 2) listę zasobów, o ile to konieczne, zatwierdza Przedstawiciel Sądu i przekazuje Podmiotowi Zewnętrznemu;
 - 3) Podmiot Zewnętrzny zobowiązuje się do wykorzystywania wyłącznie ustalonych zasobów, nawet jeśli dla sesji zdalnej dostępne są zasoby inne, niż tylko wymagane dla realizacji powierzonych zadań;
 - 4) Podmiot Zewnętrzny zobowiązuje się do niepodejmowania jakichkolwiek czynności zmierzających do penetrowania zasobów sieci Sądu.
12. Zabrania się dostępu zdalnego do Systemu Informatycznego Sądu z komputerów lub sieci dostępnych publicznie np. kafejki internetowe, dworce PKP, restauracje, bezprzewodowe sieci miejskie.
 13. Logowanie do Systemu Informatycznego Sądu za pośrednictwem łącza VPN odbywa z wykorzystaniem uwierzytelniania typu 2FA (Two-factor authentication) dostarczonego przez Sąd indywidualnie dla każdej osoby otrzymującej dostęp zdalny.

§ 11 Zasady dostępu zdalnego dla Wykonawców lub pracowników innych Jednostek Resortu, którzy uzyskują dostęp do zasobów sieciowych tych Jednostek za pośrednictwem łącza VPN Sądu

1. Dostęp zdalny dla Wykonawców lub pracowników innych Jednostek Resortu, którzy uzyskują za pośrednictwem łącza VPN Sądu dostęp do zasobów sieciowych innych Jednostek Resortu, możliwy jest tylko po spełnieniu warunków wymienionych w niniejszym paragrafie.
2. Wykonawcy i pracownicy innych Jednostek Resortu mający otrzymać dostęp zdalny do zasobów sieciowych tych Jednostek Resortu za pośrednictwem łącza VPN Sądu muszą spełnić następujące warunki:
 - 1) zapoznać się z niniejszym Regulaminem i przestrzegać jego postanowień oraz
 - 2) złożyć oświadczenie stanowiące Załącznik nr 1 do niniejszego Regulaminu do Kierownika tej Jednostki Resortu, do której zasobów mają otrzymać dostęp zdalny za pośrednictwem łącza VPN Sądu.
3. Kierownik Jednostki Resortu wnioskuję za pośrednictwem Service Desk do Dyrektora Sądu Apelacyjnego we Wrocławiu o nadanie dostępu zdalnego do zasobów sieciowych tej Jednostki za pośrednictwem łącza VPN Sądu. Wniosek musi zawierać listę osób, którym ma być nadany dostęp za pośrednictwem łącza VPN. Wzór listy stanowi załącznik nr 3. Lista powinna zawierać login AD pracownika.
4. Dyrektor Sądu Apelacyjnego we Wrocławiu może nie wyrazić zgody na wykorzystanie łącza VPN Sądu w celu uzyskania dostępu zdalnego do zasobów sieciowych innych Jednostek Resortu.
5. Wnioski obsługiwane są przez kadrę informatyczną Sądu.

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

6. Podczas rejestracji ww. osób na potrzeby nadania dostępu za pośrednictwem łącza VPN nadawany jest unikalny identyfikator oraz ustawiane jest unikalne: PIN i hasło tymczasowe niezbędne do pierwszego logowania celem uzyskania połączenia za pomocą łącza VPN Sądu.
7. Dane uwierzytelniające przekazywane są indywidualnie poszczególnym osobom, którym nadano dostęp zdalny.
8. Administrator Bezpieczeństwa Systemu Informatycznego Sądu (dalej również: ABSI) lub osoba przez niego wskazana prowadzi wykaz osób posiadających dostęp zdalny za pośrednictwem łącza VPN Sądu.
9. Sąd udziela dostępu zdalnego pracownikom Wykonawcy na czas wskazany we wniosku, jednak nie dłużej niż 12 miesięcy, zaś pracownikom innych Jednostek Resortu na czas świadczenia pracy.
10. Na kadrze informatycznej spoczywa obowiązek ograniczenia zasobów dostępnych dla sesji zdalnej (udostępnianych wykonawcom lub pracownikom za pomocą łącza VPN Sądu) do niezbędnego minimum oraz zapewnienia bezpieczeństwa danych i aktywów tej jednostki w oparciu o zasady bezpieczeństwa informacji obowiązujące w tej Jednostce Resortu.
11. Zabrania się dostępu zdalnego do zasobów sieciowych innych jednostek z komputerów lub sieci dostępnych publicznie np. kafejki internetowe, dworce PKP, restauracje, bezprzewodowe sieci miejskie.
12. Sąd Apelacyjny we Wrocławiu nie ponosi odpowiedzialności za szkody wyrządzone przez osoby, które uzyskały dostęp zdalny do zasobów sieciowych innych Jednostek Resortu za pomocą łącza VPN Sądu.
13. Logowanie za pośrednictwem łącza VPN odbywa z wykorzystaniem uwierzytelniania typu 2FA (Two-factor authentication) dostarczonego przez Sąd indywidualnie dla każdej osoby otrzymującej dostęp zdalny.
14. Pracownicy innych Jednostek Resortu, którzy w ramach struktury organizacyjnej centralnych sądowych systemów teleinformatycznych (np. ZSRK) realizują zadania na rzecz kilku lub wszystkich Jednostek Resortu otrzymują dostęp zdalny do tych zasobów na wniosek osób uprawnionych do wnioskowania o taki dostęp (uprawnienia wynikające ze struktury organizacyjnej systemu lub dokumentacji bezpieczeństwa).

§ 12 Wymagania zabezpieczeń

1. Zasady zabezpieczeń stacji roboczych Podmiotu Zewnętrznego są następujące:
 - 1) do Systemu Informatycznego Sądu mogą być podłączane wyłącznie komputery i urządzenia zgodne z minimalnymi wymaganiami bezpieczeństwa, w szczególności urządzenie:
 - a) posiada zainstalowany system antywirusowy, jego sygnatury są aktualne i aktualizowane w odstępach czasu przewidzianych przez producenta;
 - b) system operacyjny posiada zainstalowane wszystkie dostępne aktualizacje zabezpieczeń i jest zainstalowany w wersji wspieranej przez producenta oraz aktualizowany w odstępach czasu przewidzianych przez producenta;
 - c) firewall jest uruchomiony w systemie operacyjnym i posiada właściwą konfigurację, odpowiadającą wykonywanym obowiązkom pracowniczym przez użytkowników komputera.
2. Podmiot Zewnętrzny stosuje zabezpieczenia kryptograficzne zgodnie z poniższymi zasadami:
 - 1) w celu ochrony poufności przesyłanych oraz przechowywanych danych Sądu należy stosować

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

zabezpieczenia kryptograficzne;

- 2) miejsca stosowania kryptografii powinny być zgodne z wymaganiami prawnymi oraz regulacjami wewnętrznymi stosowanymi przez Sąd i udostępnionymi Podmiotowi Zewnętrznemu, w szczególności należy stosować zabezpieczenia kryptograficzne:
 - a) na dyskach twardych komputerów przenośnych,
 - b) na pendrive'ach,
 - c) na nośnikach kopii zapasowych przechowywanych poza Systemem Informatycznym Sądu,
 - d) na urządzeniach typu smartfon oraz tablet w aplikacjach, które przechowują dane objęte ochroną np. dane osobowe,
 - e) tunelach VPN,
 - f) wiadomościach poczty elektronicznej, w których przesyłane są dane objęte ochroną, w szczególności dane osobowe.
3. Zabezpieczenia kryptograficzne muszą obejmować minimum dane osobowe znajdujące się/wydostające się poza System Informatyczny Sądu.
4. Rozwiązania kryptograficzne powinny wykorzystywać następujące algorytmy:
 - 1) symetryczny szyfr blokowy AES o długości klucza min. 128-bit;
 - 2) równoważne do AES algorytmy szyfrowania, np.: Twofish, Serpent;
 - 3) kryptograficzne funkcje skrótu SHA-2, SHA-3, Whirlpool;
 - 4) asymetryczny algorytm Rivest–Shamir–Adleman – RSA;
 - 5) protokół wymiany kluczy Diffie-Hellmann – DH;
 - 6) asymetryczny algorytm Digital Signature Algorithm – DSA;
 - 7) asymetryczny algorytm ElGamal.

§ 13 Reagowanie na incydenty

1. Podmiot Zewnętrzny uzyskujący dostęp do Systemu Informatycznego Sądu zobowiązany jest niezwłocznie zgłosić Przedstawicielowi Sądu każde naruszenie bezpieczeństwa informacji kanałami wskazanymi w zapisach łączącej strony umowy albo ustaleniach pomiędzy Przedstawicielami Sądu i Podmiotu Zewnętrznego, w szczególności telefonicznie lub w formie wiadomości elektronicznej, adekwatnie do zaistniałej sytuacji.
2. Jeśli zdarzenie jest oczywistym naruszeniem bezpieczeństwa, Przedstawiciel Sądu informuje Kierownika Oddziału Informatycznego i Administratora Systemu, który może dokonać natychmiastowego odebrania uprawnień Podmiotom Zewnętrznym, w takim wypadku bez zbędnej zwłoki przekazuje informację o blokadzie dostępu Podmiotowi Zewnętrznemu.

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

3. Podmiot Zewnętrzny oraz Sąd zabezpieczają ślady (np. logi systemowe) naruszenia bezpieczeństwa w taki sposób, aby mogły stanowić dowód w sprawie.
4. W szczególnych przypadkach, o zaistniałej sytuacji poinformowane zostają organy ścigania, a w przypadku naruszenia ochrony danych osobowych, odpowiednie organy wynikające z przepisów o ochronie danych osobowych. Decyzję taką podejmuje Prezes lub Dyrektor Sądu, w zakresie swoich kompetencji.
5. Przedstawiciel Sądu we współpracy z Podmiotem Zewnętrznym sporządza notatkę dotyczącą naruszenia bezpieczeństwa lub zobowiązuje Podmiot Zewnętrzny do jej sporządzenia, określając przy tym zakres tej notatki i termin jej przedstawienia. Notatka sporządzana przez Podmiot Zewnętrzny musi być podpisana przez przedstawiciela Podmiotu Zewnętrznego lub osobę wskazaną do realizacji umowy.
6. Ostatnim etapem obsługi incydentu naruszenia bezpieczeństwa jest usunięcie skutków naruszenia bezpieczeństwa oraz wprowadzenie odpowiednich zabezpieczeń (np. poprzez zmianę konfiguracji).
7. Podmiot Zewnętrzny współpracuje z Sądem na każdym etapie postępowania z incydemem. W przypadku, w którym doszło do naruszenia ochrony danych osobowych, Podmiot Zewnętrzny współpracuje również z inspektorem ochrony danych wyznaczonym w Sądzie.
8. W przypadku osób, które uzyskują dostęp zdalny do zasobów sieciowych innych jednostek za pośrednictwem łącza VPN Sądu Apelacyjnego we Wrocławiu, zasady postępowania z incydentami określają te inne Jednostki Resortu.

§ 14 Odpowiedzialność

1. Każdy ponosić może odpowiedzialność karną przewidzianą w przepisach o ochronie danych osobowych (m.in. art. 107 ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2018 poz. 1000 ze zm.) i kodeksie karnym (m.in. Rozdziału XXXIII Kodeksu Karnego – Przestępstwa przeciwko ochronie informacji) za naruszenie ochrony danych osobowych i naruszenie bezpieczeństwa informacji.

§ 15 Postanowienia końcowe

1. Za nadzór nad przestrzeganiem postanowień Regulaminu odpowiada:
 - 1) ze strony Podmiotu Zewnętrznego odpowiednio Przedstawiciel Wykonawcy albo Kierownik innej Jednostki Resortu;
 - 2) ze strony Sądu Apelacyjnego we Wrocławiu ABSI oraz Przedstawiciel Sądu.
2. W przypadku naruszenia zapisów Regulaminu Podmiot Zewnętrzny może podlegać sankcjom dyscyplinarnym, karnym lub cywilnym, w tym wynikającym z przepisów o ochronie danych osobowych oraz innych przepisów dotyczących:
 - a) przedmiotu umowy, na podstawie której realizowane są prace, lub
 - b) powierzonych na podstawie odrębnych przepisów czynności.
3. Ewentualne odstępstwa od reguł określonych w niniejszym Regulaminie możliwe są w przypadku, w którym zasady te są odrębnie uregulowane w dokumentacji bezpieczeństwa Systemu Informatycznego Sądu. Dotyczy to w szczególności reguł obowiązujących pracowników innych Jednostek Resortu realizujących powierzone w Centralnych Systemach Informatycznych czynności (np. ZSRK).

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

4. W przypadkach nieuregulowanych decyzję podejmuje Dyrektor Sądu Apelacyjnego we Wrocławiu.

§ 16 Lista dokumentów związanych

1. Polityka Bezpieczeństwa Informacji.
2. Polityka Bezpieczeństwa Danych Osobowych.
3. Polityka Bezpieczeństwa Systemu Informatycznego.
4. Procedura zarządzania incydentami naruszenia bezpieczeństwa.
5. Dokumenty określone w ust. 2 - 4 stanowią informacje o szczególnym znaczeniu dla bezpieczeństwa i nie podlegają udostępnieniu.

§ 17 Załączniki

1. Oświadczenie (dostęp zdalny VPN).
2. Oświadczenie o zachowaniu poufności.
3. Wzór listy pracowników/podwykonawców.

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

Załącznik nr 1 do Regulaminu Ochrony Informacji dla Podmiotu Zewnętrznego Sądu Apelacyjnego we Wrocławiu – wzór oświadczenia dla osoby uzyskującej dostęp do zasobów teleinformatycznych za pośrednictwem łącza VPN Sądu Apelacyjnego we Wrocławiu.

OŚWIADCZENIE (dostęp zdalny/VPN)

osoby na potrzeby uzyskania dostępu do zasobów teleinformatycznych za pośrednictwem łącza VPN Sądu Apelacyjnego we Wrocławiu

Ja (UZUPEŁNIĆ DRUKOWANYMI LITERAMI)

numer telefonu komórkowego¹..... (UZUPEŁNIĆ DRUKOWANYMI LITERAMI)

służbowy imienny adres poczty elektronicznej.....(UZUPEŁNIĆ DRUKOWANYMI LITERAMI)

niżej podpisany, niniejszym:

- Potwierdzam, że zostałem zapoznany z Regulaminem Ochrony Informacji dla Podmiotu Zewnętrznego oraz zobowiązuję się do ścisłego przestrzegania jego zapisów.
- Za pośrednictwem VPN Sądu Apelacyjnego we Wrocławiu uzyskuję dostęp do systemu informatycznego Sądu Apelacyjnego we Wrocławiu/do zasobów sieciowych innych jednostek Resortu za pośrednictwem łącza VPN².
- Oświadczam, że:
 - Dostęp do Systemu Informatycznego Sądu (zwany dalej: Systemem) będzie wykorzystywany przeze mnie do realizacji zadań polegających na (wskazać cel dostępu, np.: wsparcie, utrzymanie) wynikających z umowy nr.....z dnia...../wniosku Kierownika Jednostki³* ... z dnia ... (znak sprawy ...).
 - System operacyjny, z jakiego będą nawiązywane połączenia VPN posiada zainstalowane najnowsze aktualizacje systemowe oraz posiada uruchomionego i aktualizowanego automatycznie antywirusa⁴.
 - Wiadomo mi, że wszelkie informacje uzyskane w związku z dostępem do Systemu, w tym dane osobowe i sposoby ich zabezpieczenia, są poufne i zobowiązuje się do zachowania ich w tajemnicy, zarówno w trakcie posiadania dostępu do systemu jak i po jego wygaśnięciu.
 - Zobowiązuję się do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. regulacji oraz przed nieautoryzowaną ich zmianą, utratą, uszkodzeniem lub zniszczeniem.

¹ W przypadku Wykonawców.

² Wybrać właściwe.

³ Uzupełnić.

⁴ W przypadku pracowników innych Jednostek Resortu możliwe jest złożenie tego oświadczenia przez Kierownika Jednostki.

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

- e) Jestem świadomy/-a, że ponoszę pełną odpowiedzialność za działania przeprowadzone w Systemie.
 - f) Przyjmuję do wiadomości że nie wolno mi wykonywać żadnych działań na systemach produkcyjnych bez zgody zleceniodawcy lub kierownika Jednostki Resortu, w której działania mają zostać wykonane, przy czym ewentualne odstępstwa od tej reguły muszą być przewidziane w strukturze organizacyjnej lub dokumentacji bezpieczeństwa Systemu (np. ZSRK).
 - g) Zobowiązuję się do występowania o nadanie uprawnień tylko do Systemów / modułów Systemu, do których są one niezbędne w celu wykonania powierzonych zadań. Zobowiązuję się również do niewystępowania o uprawnienia do systemów produkcyjnych, jeśli nie jest to bezwzględnie konieczne do zrealizowania zlecenia.
 - h) Zobowiązuję się do występowania o nadanie uprawnień na okres nie dłuższy, niż niezbędny do realizacji powierzonych zadań.
 - i) Zobowiązuję się do wykorzystywania tylko i wyłącznie ustalonych zasobów Systemu, nawet, jeśli dostępne są inne, niż tylko wymagane do realizacji powierzonych zadań.
 - j) Nie będę podejmować jakichkolwiek prób ingerencji w System, poza czynnościami związanymi z realizacją celu wskazanego w lit. a oświadczenia.
 - k) Nie będę omijać mechanizmów kontroli i zabezpieczeń Systemu.
 - l) Nie będę udostępniać innym osobom dostępu do Systemu (login, hasło).
 - m) Nie będę pozyskiwać, gromadzić i przechowywać danych z Systemu, jeśli nie jest to niezbędne do realizacji powierzonych zadań.
4. Przyjmuję do wiadomości, że w przypadku uszkodzenia jakiegokolwiek z udostępnionych zasobów Systemu lub wprowadzenia nieautoryzowanych zmian, Sąd lub inna Jednostka Resortu może dochodzić naprawienia szkody w myśl obowiązujących przepisów prawa, w tym prawa cywilnego, ja zaś mogę podlegać odpowiedzialności dyscyplinarnej i karnej na podstawie obowiązujących przepisów prawa.

.....
(data, czytelny podpis składającego oświadczenie)

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

Załącznik nr 2 do Regulaminu Ochrony Informacji dla Podmiotu Zewnętrznego Sądu Apelacyjnego we Wrocławiu – wzór oświadczenia o zachowaniu poufności

Oświadczenie o zachowaniu poufności (pracownicy innych Jednostek Resortu)

.....

Imię i Nazwisko (UZUPEŁNIĆ DRUKOWANYMI LITERAMI)

.....

Stanowisko (UZUPEŁNIĆ DRUKOWANYMI LITERAMI)

.....

Jednostka i Komórka organizacyjna (UZUPEŁNIĆ DRUKOWANYMI LITERAMI)

Ja niżej podpisany/podpisana

1. Oświadczam, że znane są mi przepisy:

- a) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000 ze zm.),
- b) ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125);
- c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r. (Dz.Urz.UE.L Nr 119, str. 1 ze zm.).

2. Zobowiązuję się do:

- a) zachowania w tajemnicy, także po zakończeniu współpracy z Sądem, informacji i danych osobowych, do których będę mieć dostęp,
- b) wykorzystywania informacji i danych osobowych jedynie w celach, w których zostały mi przekazane podczas wykonywania przeze mnie zadań lub obowiązków służbowych (*odpowiednio: odbywania stażu, praktyki, innych*)⁵,
- c) zachowania w tajemnicy, także po zakończeniu współpracy z Sądem Apelacyjnym we Wrocławiu, sposobów zabezpieczenia danych osobowych stosowanych przy ich przetwarzaniu, o ile nie są one powszechnie znane lub nie wynikają w sposób oczywisty z innych powszechnie znanych informacji,
- d) zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed: udostępnieniem osobom nieupoważnionym, zabraniami przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. regulacji oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,

⁵ Uzupełnić lub niepotrzebne skreślić.

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

- e) niezwłocznego powiadomienia Administratora Danych Osobowych w Sądzie Apelacyjnym we Wrocławiu o każdorazowym podejrzeniu lub stwierdzeniu próby lub faktu naruszenia ochrony danych osobowych, bezpieczeństwa danych osobowych lub innych informacji Sądu przetwarzanych w sposób tradycyjny jak i w systemach informatycznych.

3. Potwierdzam, że zostałem/am zapoznany/a z Regulaminem Ochrony Informacji dla Podmiotu Zewnętrznego zrozumiałem/am jego treść oraz zobowiązuję się do ścisłego przestrzegania jego zapisów⁶.

4. Przyjmuję do wiadomości, że postępowanie sprzeczne z powyższymi zobowiązaniami może skutkować sankcjami dyscyplinarnymi, a także odpowiedzialnością karną przewidzianą w przepisach o ochronie danych osobowych (m.in. art. 107 ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2018 poz. 1000 ze zm.) i kodeksie karnym (m.in. Rozdziału XXXIII Kodeksu Karnego – Przestępstwa przeciwko ochronie informacji).

.....

Miejscowość , data

.....

podpis (imię i nazwisko; czytelnie)

Załącznik nr 3 do Regulaminu Ochrony Informacji dla Podmiotu Zewnętrznego Sądu Apelacyjnego we Wrocławiu –
Wzór listy pracowników, w tym podwykonawców

⁶ Uzupełnić lub niepotrzebne skreślić.

SA Wrocław		Wersja 2.2
	Regulamin Ochrony Informacji dla Podmiotu Zewnętrznego	Rok wydania: 2026

LP	Nazwa Wykonawcy / Jednostki Resortu	Imię	Nazwisko	Imienny, służbowy adres e-mail	Identyfikator w Systemie (opcjonalnie)	numer telefonu komórkowego (opcjonalnie, wymagany przy VPN dla Wykonawcy)	PESEL (opcjonalnie dla Wykonawcy, może być wymagany przy nadawaniu dostępu do niektórych systemów)
1							
2							
3							