UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

§1 Postanowienia ogólne

1. Umowa Powierzenia stanowi integralną część Umowy, Regulaminu Usługi Sklepu Internetowego i Polityki Prywatności oraz określa zasady przetwarzania przez Operatora na zlecenie Klienta danych osobowych za pośrednictwem Oprogramowania Operatora.
2. Umowa Powierzenia stanowi całość zobowiązań oraz warunków powierzenia przetwarzania danych osobowych pomiędzy Klientem i Operatorem w związku z realizacją usług i korzystaniem przez Klienta z Oprogramowania Operatora.

§2 Definicje

1) Użyte sformułowania oznaczają:
   a) **Administrator Danych –** oznacza Klienta lub Podmiot Powiązany, który samodzielnie lub wspólnie z innymi podmiotami ustala cele i sposoby przetwarzania Danych Osobowych;
   b) **Audyt –** oznacza sprawdzenie (w tym inspekcję) zgodności przetwarzania Danych Osobowych za pośrednictwem Oprogramowania Operatora z przepisami prawa, w szczególności z RODO oraz Umową Powierzenia, z wyłączeniem: (i) informacji zawierających tajemnicę przedsiębiorstwa lub (ii) przeprowadzania testów penetracyjnych lub innych podobnych testów Oprogramowania Operatora. Audyt może być dokonany samodzielnie przez Klienta lub za pośrednictwem upoważnionego przez niego audytora, po przedłożeniu przez audytora pełnomocnictwa do działania w imieniu Klienta, przy czym Audyt nie powinien być wykonywany przez konkurenta (w rozumieniu przepisów o ochronie konkurencji) Operatora;
   c) **Cel Przetwarzania –** oznacza realizację przez Operatora zobowiązań określonych w Umowie w związku ze świadczeniem na rzecz Klienta usług;
   d) **Czynności Przetwarzania –** oznaczają wszelkie operacje na Danych Osobowych, które będzie wykonywał Podmiot Przetwarzający na polecenie Administratora Danych;
   e) **Dalszy Podmiot Przetwarzający –** oznacza podmiot, z którego usług korzysta Podmiot Przetwarzający przy wykonywaniu praw i obowiązków określonych w Umowie o świadczenie Usług i dokonywania konkretnych Czynności Przetwarzania, który będzie miał dostęp do Danych Osobowych;
   f) **Dane Osobowe –** oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, których dotyczy powierzenie przetwarzania na mocy Umowy Powierzenia;
   g) **EOG –** oznacza Europejski Obszar Gospodarczy zdefiniowany w Porozumieniu o Europejskim Obszarze Gospodarczym (Dz. U. UE L z dnia 3 stycznia 1994 r. ze zm.), czyli państwa należące do Unii Europejskiej oraz Norwegię, Islandię i Lichtenstein;

h) **Klient** – oznacza przedsiębiorcę, z którym Operator bezpośrednio lub za pośrednictwem Użytkownika zawarł Umowę;
i) **Naruszenie Ochrony Danych Osobowych** – oznacza naruszenie bezpieczeństwa Danych Osobowych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych Osobowych, w stosunku do których są wykonywane Czynności Przetwarzania przez odpowiednio Podmiot Przetwarzający lub Dalszy Podmiot Przetwarzający;
j) **Ocena Skutków dla Ochrony Danych** – oznacza ocenę skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych, o której mowa w art. 35-36 RODO;
k) **Operator** – oznacza spółkę AM GLOBAL SOLUTIONS spółka z ograniczoną odpowiedzialnością z siedzibą w Łodzi (adres: ul. Henryka Sienkiewicza 59, 90-009 Łódź), zarejestrowana w rejestrze przedsiębiorców prowadzonym przez Sąd Rejonowy dla m.st. Warszawy w Warszawie XIV Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000645598, NIP: 5342532004, REGON: 365810667;
l) **Oprogramowanie** – program komputerowy w rozumieniu Ustawy z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych, służący do prowadzenia Sklepu Internetowego, udostępniany Administratorowi Sklepu przez Usługodawcę w ramach Usługi Sklepu Internetowego;
m) **Organ Nadzorczy** – oznacza Prezesa Urzędu Ochrony Danych Osobowych;
n) **Podmiot Przetwarzający** – oznacza Operatora, który przetwarza Dane Osobowe na wyraźne polecenie Klienta;
o) **Umowa** – oznacza umowę o świadczenie usług przy pomocy Oprogramowania;
p) **Użytkownik** – oznacza osobę korzystająca z Oprogramowania, prowadzącą działalność gospodarczą lub działająca w imieniu Klienta;
q) **RODO** – oznacza rozporządzenie 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);
r) **Sprzeciw** – oznacza sprzeciw Klienta wobec dalszego powierzenia przetwarzania Danych Osobowych przez Operatora Dalszemu Podmiotowi Przetwarzającemu. Sprzeciw wymaga zachowania formy pisemnej pod rygorem nieważności.

2) Wszystkie pojęcia pisane z wielkiej litery, a niezdefiniowane w ust. 1 powyżej, mają znaczenia nadane im w Regulaminie Serwisu lub Regulaminie Usługi Sklepu Internetowego. W przypadku rozbieżności pomiędzy definicją pojęcia zawartą w Regulaminie, a definicją w Regulaminie Serwisu, zastosowanie mają znaczenia wskazane w ust. 1 powyżej.

§3 Dane Osobowe

Czynności Przetwarzania	Rodzaj Danych Osobowych	Kategoria osób, których Dane Osobowe dotyczą	Kategorie Danych Osobowych
Udostępnienie i utrzymywanie zdalnej platformy programistycznej do prowadzenia sklepu internetowego	imię, nazwisko, id, email, numer telefonu, hasło, adres zamieszkania	Pracownicy, współpracownicy, klienci, kontrahenci, potencjalni klienci, użytkownicy Sklepu Internetowego	Dane zwykłe
Dostarczenie usługi wsparcia technicznego w ramach usługi Sklepu Internetowego.	imię, nazwisko, id, email, numer telefonu, hasło, adres zamieszkania	Pracownicy, współpracownicy, klienci, kontrahenci, potencjalni klienci, użytkownicy Sklepu Internetowego	Dane zwykłe
Obsługa żądań osób, których dane dotyczą	imię, nazwisko, email, numer telefonu, adres zamieszkania, adres zameldowania, PESEL, nr dowodu osobistego, *inne dane udostępnione przez osobę, której dane dotyczą*	Pracownicy, współpracownicy, klienci, kontrahenci, potencjalni klienci, użytkownicy Sklepu Internetowego	Dane zwykłe, dane szczególne
Współpraca z podmiotami przetwarzającymi dane (administrator, współadministrator, procesor)	imię, nazwisko, id, email, numer telefonu	Przedstawiciele administratora, współadministratora, procesora	Dane zwykłe, dane szczególne

§4 Przedmiot i czas trwania przetwarzania Danych Osobowych

1. Klient powierza Operatorowi przetwarzanie Danych Osobowych w związku z Umową, a Operator przyjmuje Dane Osobowe do przetwarzania.

2. Operator może przetwarzać Dane Osobowe wyłącznie w celu wykonania zobowiązań wynikających z Umowy, w tym zapewnienia określonych funkcjonalności oraz wsparcia technicznego Oprogramowania Operatora.
3. Operator może przetwarzać Dane Osobowe wyłącznie przez okres: (i) obowiązywania Umowy oraz (ii) od rozwiązania lub wygaśnięcia Umowy do czasu usunięcia Danych Osobowych zgodnie z postanowieniami Umowy Powierzenia, chyba że Klient oraz Operator ustalą inny okres przetwarzania Danych Osobowych w drodze odrębnego porozumienia.
4. Operator będzie przetwarzał Dane Osobowe na udokumentowane polecenie Klienta. Przez udokumentowane polecenie należy rozumieć przetwarzanie zgodne z niniejszą umową, jak również polecenia wydane w formie pisemnej lub elektronicznej (poczta elektroniczna).
5. Umowa Powierzenia rozwiązuje się z chwilą rozwiązania Umowy.

§5 Środki techniczne i organizacyjne

1. Uwzględniając stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania Danych Osobowych oraz ryzyko naruszenia praw i wolności osób, których Dane Osobowe dotyczą, Operator zapewni adekwatne do rodzaju Danych Osobowych oraz ryzyka naruszenia praw i wolności środki techniczne i organizacyjne przetwarzania Danych Osobowych. Minimalne środki techniczne i organizacyjne przetwarzania Danych Osobowych zostały określone w **Załączniku nr 1** do Umowy Powierzenia.
2. Operator dopuści do przetwarzania Danych Osobowych wyłącznie osoby działające z jego upoważnienia, których dostęp do Danych Osobowych jest niezbędny do wykonania usług określonych w Umowie.
3. Operator zapewni, aby osoby działające z jego upoważnienia i mające dostęp do Danych Osobowych zostały odpowiednio przeszkolone, w tym zostały zapoznane z przepisami dotyczącymi ochrony Danych Osobowych i odpowiedzialnością za ochronę Danych Osobowych przed niepowołanym dostępem, nieuzasadnioną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem Danych Osobowych.
4. Operator zobowiąże osoby działające z jego upoważnienia i mające dostęp do Danych Osobowych do zachowania tajemnicy odnośnie przetwarzanych Danych Osobowych.

§6 Dalsze Podmioty Przetwarzające

1. Stosownie do treści art. 28 ust. 2 RODO Klient wyraża zgodę na korzystanie przez Operatora z usług Dalszych Podmiotów Przetwarzających przy przetwarzaniu Danych Osobowych, w celu prawidłowego świadczenia usług.
2. Lista Dalszych Podmiotów Przetwarzających, z których Operator na dzień rozpoczęcia obowiązywania Umowy Powierzenia korzysta lub zamierza korzystać znajduje się w **Załączniku nr 2** do Umowy Powierzenia. Zawierając Umowę Powierzenia Klient akceptuje powierzenie przetwarzania Danych Osobowych podmiotom określonym w **Załączniku nr 2** do Umowy Powierzenia.
3. Operator poinformuje Klienta o zamiarze skorzystania z usług innego Dalszego Podmiotu Przetwarzającego na co najmniej 14 dni przed rozpoczęciem korzystania z usług danego Dalszego Podmiotu Przetwarzającego. Informacja o Dalszym Podmiocie Przetwarzającym

zostanie przekazana na adres poczty elektronicznej Klienta. Nowy Dalszy Podmiot Przetwarzający zostanie uwzględniony w zmienionej treści Załącznika nr 2. Zmiana **Załącznika nr 2** nie wymaga zmiany Umowy Powierzenia.

4. W terminie 7 dni od dnia otrzymania informacji o Dalszym Podmiocie Przetwarzającym, Klient może zgłosić Sprzeciw wobec Dalszego Podmiotu Przetwarzającego.
5. W przypadku zgłoszenia Sprzeciwu, Operatorowi przysługuje możliwość zaproponowania innego Dalszego Podmiotu Przetwarzającego. Zgłoszenie Sprzeciwu co do innego Dalszego Podmiotu Przetwarzającego oznacza wypowiedzenie Umowy ze skutkiem na koniec miesiąca następującego po miesiącu, w którym złożono Sprzeciw. W czasie trwania okresu wypowiedzenia Umowy, Operator nie przekaże innemu Dalszemu Podmiotowi Przetwarzającemu Danych Osobowych do przetwarzania.
6. W przypadku korzystania przez Operatora z usług Dalszego Podmiotu Przetwarzającego, Operator zawiera z Dalszym Podmiotem Przetwarzającym umowę, która nakłada na Dalszy Podmiot Przetwarzający takie same obowiązki ochrony danych jak określone w Umowie Powierzenia. Umowa z Dalszym Podmiotem Przetwarzającym w szczególności zawiera zobowiązania dotyczące przestrzegania przepisów RODO, w tym zobowiązania dotyczące stosowania środków technicznych i organizacyjnych przetwarzania Danych Osobowych, które będą adekwatne do rodzaju powierzonych Danych Osobowych oraz ryzyka naruszenia praw osób, których Dane Osobowe dotyczą. Uprawnienia Dalszych Podmiotów Przetwarzających nie będą szersze niż uprawnienia Operatora określone w Umowie Powierzenia.
7. Operator ponosi odpowiedzialność za działania i zaniechania Dalszych Podmiotów Przetwarzających zgodnie z zasadami odpowiedzialności określonymi w § 11 Umowy Powierzenia.

§7 Wsparcie Klienta

Uwzględniając charakter wykonywanych Czynności Przetwarzania Danych Osobowych oraz dostępne informacje w związku ze świadczeniem Usług, Operator zapewni Klientowi pomoc w wywiązaniu się z następujących obowiązków:

a) zapewnienia odpowiednich środków technicznych i organizacyjnych przetwarzania Danych Osobowych przez zastosowanie środków technicznych i organizacyjnych określonych w §5 Umowy Powierzenia;
b) przeprowadzenia Oceny Skutków dla Ochrony Danych przez udzielanie Klientowi niezbędnych informacji odnośnie do przetwarzania Danych Osobowych w Oprogramowaniu, potrzebnych do przeprowadzenia przez Klienta Oceny Skutków dla Ochrony Danych;
c) udzielania odpowiedzi na żądania osób, których Dane Osobowe dotyczą, w zakresie określonym w art. 15-22 RODO, przez zapewnienie Klientowi, na jego żądanie, zgłoszone na adres: kontakt@polminuty.pl następujących możliwości: (i) eksportu Danych Osobowych, (ii) usunięcia i ograniczenia przetwarzania Danych Osobowych oraz (iii) sprostowania Danych Osobowych. W przypadku zgłoszenia przez osobę, której Dane Osobowe dotyczą, żądania bezpośrednio do Operatora jako Podmiotu Przetwarzającego Dane Osobowe, Operator poinformuje Klienta niezwłocznie o zgłoszonym żądaniu i ustali z nim sposób postępowania w stosunku do zgłoszonego żądania;

d) zgłoszenia Naruszenia Ochrony Danych Osobowych Organowi Nadzorczemu oraz z obowiązku zawiadomienia osób, których Dane Osobowe dotyczą, o Naruszeniu Ochrony Danych Osobowych zgodnie z art. 33-34 RODO.

§8 Naruszenie Ochrony Danych Osobowych

1. Operator zgłasza Klientowi Naruszenia Ochrony Danych Osobowych niezwłocznie, jednakże nie później niż w terminie 36 godzin od jego stwierdzenia.
2. Zgłoszenie zawiera:
   a) opis okoliczności zdarzenia stanowiącego Naruszenie Ochrony Danych Osobowych oraz jego ustalonych lub podejrzewanych przyczyn;
   b) opis charakteru Naruszenia Ochrony Danych Osobowych, w tym, w miarę możliwości wskaże kategorie i przybliżoną liczbę osób, których Dane Osobowe dotyczą oraz kategorie i przybliżoną liczbę wpisów Danych Osobowych, których dotyczy Naruszenie Ochrony Danych Osobowych;
   c) opis możliwych konsekwencji Naruszenia Ochrony Danych Osobowych;
   d) opis zastosowanych przez Operatora środków zaradczych w celu zminimalizowania ewentualnych negatywnych skutków Naruszenia Ochrony Danych Osobowych.
3. Informacja o Naruszeniu Ochrony Danych Osobowych zostanie przekazana przez Operatora na adres poczty elektronicznej wskazany przez Klienta przy rejestracji.
4. Operator w przypadku stwierdzenia Naruszenia Ochrony Danych Osobowych podejmuje niezwłocznie niezbędne środki techniczne i organizacyjne w celu zaradzenia Naruszeniu Ochrony Danych Osobowych i zminimalizowaniu jego ewentualnych negatywnych konsekwencji.

§9 Przekazywanie informacji

1. Operator niezwłocznie poinformuje Klienta o:
   a) wszelkich postępowaniach, w szczególności administracyjnych lub sądowych, dotyczących przetwarzania Danych Osobowych, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu sądowym dotyczących Danych Osobowych, skierowanych do Operatora, a także o wszelkich planowanych postępowaniach lub o realizowanych kontrolach dotyczących przetwarzania Danych Osobowych;
   b) poleceniach wydanych przez Klienta Operatora dotyczących przetwarzania Danych Osobowych, które zdaniem Operatora stanowią naruszenie przepisów RODO lub innych przepisów prawa o ochronie danych osobowych.
2. Operator na żądanie Klienta udostępni Klientowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.
3. Informacje zostaną przekazane na adres poczty elektronicznej Klienta.

§10 Audyty

1. Klient jest uprawniony do przeprowadzenia Audytu w każdym czasie. W szczególności Klient jest uprawniony do przeprowadzenia Audytu w następujących przypadkach: (i) obowiązek przeprowadzenia Audytu został nałożony przez Organ Nadzorczy lub (ii)

przeprowadzenie Audytu jest konieczne dla wyjaśnienia Naruszenia Ochrony Danych Osobowych.

2. Klient jest zobowiązany zawiadomić Operatora o zamiarze przeprowadzenia Audytu co najmniej na 7 dni roboczych przed planowaną datą rozpoczęcia Audytu. Zawiadomienie powinno wskazywać dokładny zakres, termin oraz osoby upoważnione przez Klienta do przeprowadzenia Audytu i zostać doręczone na adres poczty elektronicznej Operatora.
3. Jeżeli przeprowadzenie Audytu w terminie wskazanym przez Klienta nie będzie możliwe, w szczególności z uwagi na liczbę Audytów zgłoszonych przez innych klientów, Operator poinformuje Klienta o pierwszym możliwym terminie przeprowadzenia Audytu. Niniejsze postanowienie nie ma zastosowania w przypadku, gdy obowiązek przeprowadzenia Audytu został nałożony przez Organ Nadzorczy lub przeprowadzenie Audytu jest konieczne dla wyjaśnienia Naruszenia Ochrony Danych Osobowych.
4. Operator ustala maksymalny czas trwania Audytu, który powinien wynosić nie dłużej niż 3 dni robocze, chyba że dłuższy czas okaże się niezbędny z uwagi na cel Audytu. W takim przypadku Strony uzgodnią maksymalny czas trwania Audytu.
5. Strony, po zakończeniu Audytu, podpisują protokół, który zawiera wnioski z Audytu, w tym uzgodniony przez Strony zakres ewentualnych zmian w zakresie przetwarzania Danych Osobowych przez Operatora.
6. Klient we własnym zakresie pokrywa koszty przeprowadzenia Audytu.
7. Operator niezwłocznie poinformuje Klienta, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii lub właściwego państwa członkowskiego dotyczących ochrony danych osobowych.

§11 Odpowiedzialność

1. Operator ponosi odpowiedzialność w przypadku niewykonania lub nienależytego wykonania Umowy Powierzenia. Operator odpowiada za szkody poniesione przez Klienta do wysokości szkody rzeczywistej, w zakresie, w jakim takie ograniczenie odpowiedzialności jest dopuszczalne w oparciu o bezwzględnie obowiązujące przepisy prawa.
2. Operator ponosi odpowiedzialność za działania lub zaniechania Dalszych Podmiotów Przetwarzających jak za własne działania lub zaniechania zgodnie z zasadami odpowiedzialności określonymi Umowie Powierzenia.

§12 Zakończenie przetwarzania Danych Osobowych

1. Po zakończeniu świadczenia usług związanych z przetwarzaniem Danych Osobowych, Operator, w zależności od decyzji Klienta, usunie lub zwróci Klientowi wszelkie Dane Osobowe oraz usunie wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazuje przechowywanie Danych Osobowych.
2. Decyzja Klienta w zakresie żądania usunięcia lub zwrotu Danych Osobowych powinna zostać doręczona Operatorowi na piśmie, pod rygorem jej bezskuteczności, w terminie nie dłuższym niż 7 dni od dnia zakończenia świadczenia usług związanych z przetwarzaniem Danych Osobowych.
3. Operator usunie lub zwróci Dane Osobowe w terminie 30 dni od dnia otrzymania pisemnej decyzji Klienta, chyba że Strony w odrębnym porozumieniu ustalą odmienny

termin usunięcia lub zwrotu Danych Osobowych. Operator potwierdzi usunięcie Danych Osobowych stosownym protokołem. Na życzenie Klienta Operator przekaże Klientowi kopię protokołu usunięcia Danych Osobowych.

4. Operator zapewni, że wszystkie Dalsze Podmioty Przetwarzające usuną Dane Osobowe na zasadach określonych w niniejszym paragrafie.
5. W przypadku, gdy Operator na podstawie przepisów prawa będzie obowiązany do przechowywania Danych Osobowych po zakończeniu świadczenia usług, Operator niezwłocznie poinformuje Klienta o wystąpieniu takich okoliczności. W takiej sytuacji Operator będzie przetwarzał Dane Osobowe wyłącznie w zakresie i celu wykonania obowiązków wynikających z przepisów prawa, a po ich spełnieniu niezwłocznie usunie Dane Osobowe.

§13 Postanowienia końcowe

1. Umowa Powierzenia podlega prawu polskiemu.
2. Spory pomiędzy Stronami rozstrzygają sądy polskie, właściwe dla siedziby powoda.
3. W sprawach nieuregulowanych w Umowie Powierzenia odpowiednie zastosowanie znajdują postanowienia Umowy i Kodeksu cywilnego oraz RODO, jak również innych aktów prawnych regulujących zasady ochrony danych osobowych.
4. W przypadku rozbieżności pomiędzy postanowieniami Umowy Powierzenia a postanowieniami Umowy, zastosowanie mają postanowienia Umowy.

ZAŁĄCZNIKI:

Załącznik nr 1	Lista środków technicznych i organizacyjnych.
Załącznik nr 2	Lista Dalszych Podmiotów Przetwarzających.

Załącznik nr 1

BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. Zabezpieczenia organizacyjne:
   a) Operator posiada Politykę Bezpieczeństwa Informacji, która reguluje zasady ochrony danych osobowych przez Operatora, w tym politykę zarządzania incydentami;
   b) Operator przeprowadza szkolenia wstępne i okresowe z ochrony danych osobowych i bezpieczeństwa informacji dla pracowników;
   c) Operator nadaje pracownikom imienne upoważnienia do przetwarzania danych osobowych. Upoważnienia są cyklicznie weryfikowane.
2. Zabezpieczenia dotyczące bezpieczeństwa fizycznego:
   a) Operator wydzielił obszary bezpieczne, w których przetwarzane są Dane Osobowe;
   b) Operator zastosował odpowiednie środki bezpieczeństwa tj. kontrolę dostępu, ochronę fizyczną, monitoring CCTV.
3. Zabezpieczenia dotyczące kontroli dostępu:
   a) każdy pracownik Operatora posiada odrębne, unikalne konto dostępowe do systemów informatycznych, w których przetwarzane są Dane Osobowe;
   b) Operator stosuje politykę silnych haseł, zmiany haseł i blokowania kont;
   c) Operator wprowadził szyfrowanie urządzeń mobilnych przetwarzających Dane Osobowe;
   d) dostęp zdalny do Danych Osobowych jest centralnie zarządzany i kontrolowany.
4. Zabezpieczenia dotyczące bezpieczeństwa operacyjnego:
   a) systemy informatyczne i Oprogramowanie Operatora służące do przetwarzania Danych Osobowych są regularnie aktualizowane, weryfikowane pod kątem podatności oraz zabezpieczone przez systemy antywirusowe;
   b) Operator stosuje ochronę przed nieuprawnionym dostępem do systemów i sieci przez zaporę ogniową (firewall);
   c) zastosowano filtrowanie dostępów do stron internetowych. Zostały wdrożone systemy monitorujące ruch sieciowy, wykryte anomalie są logowane i raportowane.

I. BEZPIECZEŃSTWO OPROGRAMOWANIA

Zabezpieczenia Systemów Operatora zostały wyselekcjonowane w oparciu o standard OWASP ASVS oraz najlepsze praktyki bezpieczeństwa.

W Systemach Operatora stosowane są następujące zabezpieczenia:

1. **Zabezpieczenia dotyczące architektury:**
   a) Oprogramowanie jest cyklicznie testowane przy pomocy testów penetracyjnych;
   b) komponenty architektury Oprogramowania są monitorowane pod kątem podatności;
   c) stosowane są zabezpieczenia sieciowe na styku z siecią Internet.
2. **Zabezpieczenia dotyczące uwierzytelniania**: jest stosowana weryfikacja tożsamości nadawcy w trakcie komunikacji zapewniająca, że tylko upoważnione podmioty mogą być uwierzytelnione, a dane uwierzytelniające są przechowywane i transportowane w sposób bezpieczny.
3. **Zabezpieczenia dotyczące zarządzania sesją**: zostały wdrożone mechanizmy zarządzania sesją, przy pomocy których interakcja z użytkownikiem jest nadzorowana i bezpieczna.

Sesje są unikalne dla każdego użytkownika i nie mogą zostać odgadnięte lub współdzielone.

4. **Zabezpieczenia dotyczące kontroli dostępu**: jest zapewniony dostęp jedynie do tych zasobów, na które wyrażono zgodę. Osoby uzyskujące dostęp posiadają ważne dane uwierzytelniające, a użytkownicy są powiązani ze zdefiniowanymi zestawami ról i uprawnień.
5. **Zabezpieczenia dotyczące obsługi złośliwych danych wejściowych**: jest stosowana walidacja danych wejściowych zapewniająca poprawność i dostosowanie do zamierzonych celów.
6. **Zabezpieczenia dotyczące nieaktywnych mechanizmów kryptograficznych**: jest zapewnione, że wszystkie moduły kryptograficzne kończące pracę niepowodzeniem robią to w sposób bezpieczny. Dostęp do kluczy jest zarządzany w bezpieczny sposób.
7. **Zabezpieczenia dotyczące obsługi i logowania błędów**: stosowane są mechanizmy logowania zdarzeń bezpieczeństwa, a wszystkie logowane informacje są obsługiwane i przechowywane w sposób bezpieczny.
8. **Zabezpieczenia dotyczące mechanizmów ochrony danych**: jest zapewniona ochrona danych przed nieautoryzowanym podglądem lub ujawnieniem, zarówno podczas transmisji jak i podczas przechowywania. Dane chronione są przed złośliwym tworzeniem, zmianą lub usuwaniem przez nieupoważnione osoby oraz dostępne są tylko dla autoryzowanych użytkowników gdy tylko są potrzebne.
9. **Zabezpieczenia dotyczące komunikacji:**
   a) stosowane jest bezpieczne połączenie we wszystkich połączeniach (zewnętrznych i wewnętrznych), które są uwierzytelniane lub związane są z wrażliwymi danymi lub funkcjami;
   b) zapewnione są mechanizmy uniemożliwiające pogorszenie parametrów bezpieczeństwa połączenia;
   c) stosowany jest najsilniejszy dostępny algorytm szyfrowania.
10. **Zabezpieczenia dotyczące konfiguracji http:** są zapewnione bezpieczne zestawy znaków w nagłówkach oraz nie są ujawniane informacje o wersjach komponentu systemów.
11. **Zabezpieczenia dotyczące bezpieczeństwa plików i zasobów**: jest zapewnione, że niezaufane dane z plików obsługiwane są w sposób bezpieczny, a pliki źródłowe otrzymane z niezaufanych źródeł są przechowywane poza katalogiem głównym z ograniczonymi uprawnieniami.
12. **Zabezpieczenia dotyczące bezpieczeństwa webservice'ów**: jest zapewniona walidacja wszystkich parametrów wejściowych, które są transmitowane z mniej do bardziej zaufanych warstw.
13. **Zabezpieczenia dotyczące bezpieczeństwa procesu konfiguracji**: jest zapewnione bezpieczeństwo podczas zmian w oprogramowaniu i wykorzystywanie aktualnych bibliotek i platform, a komunikacja pomiędzy komponentami jest szyfrowana i uwierzytelniana.

Załącznik nr 2 (Dalsze Podmioty Przetwarzające)

Lp.	Nazwa	Adres	Cel dalszego powierzenia
1.	Greener Marcin Waligórski	ul. Adama Mickiewicza 37/58 01-625 Warszawa	Dostarczanie usługi hostingu oraz kolokacji serwerów.
2.	AfterMarket.pl Limited	Chytron 3, Office 301 1075 Nicosia Cypr	Dostarczanie usług wsparcia technicznego. Obsługa postępowań reklamacyjnych.