Załącznik nr 1 do Regulaminu świadczenia usług

Polityka Dopuszczalnego Korzystania (AUP — Acceptable Use Policy)

Wersja obowiązująca od dnia 02-09-2026 r.

1. Przedmiot AUP

1. Niniejsza Polityka Dopuszczalnego Korzystania (dalej: **„AUP"**) określa zasady prawidłowego korzystania z Usług świadczonych przez CYBERMONKEY SP. Z O.O. (dalej: **„Usługodawca"**) oraz katalog działań zabronionych.
2. AUP stanowi załącznik nr 1 do Regulaminu świadczenia usług. Pojęcia użyte w AUP mają znaczenie nadane im w Regulaminie.
3. Akceptacja Regulaminu obejmuje akceptację AUP. Zmiana AUP następuje w trybie określonym w §13 Regulaminu.

2. Zasady ogólne

1. Klient zobowiązuje się korzystać z Usługi w sposób zgodny z prawem, Regulaminem, AUP, zasadami współżycia społecznego oraz w sposób niezakłócający działania infrastruktury Usługodawcy ani nieutrudniający korzystania z Usług innym Klientom.
2. Klient ponosi wyłączną odpowiedzialność za wszelkie działania podejmowane za pomocą Usługi, w tym za działania osób trzecich, którym udostępnił dane dostępowe.
3. Usługodawca zastrzega sobie prawo do aktualizacji AUP w związku ze zmianami technologicznymi, prawnymi lub organizacyjnymi.

3. Działania zabronione

Katalog poniżej ma charakter otwarty (nie wyczerpujący). Usługodawca może uznać za naruszenie AUP także działanie niewymienione wprost, wyłącznie w przypadku gdy jest ono tożsame co do charakteru i szkodliwości z wymienionymi oraz jest bezprawne albo stwarza istotne zagrożenie dla infrastruktury Usługodawcy, innych Klientów lub osób trzecich.

3.1. Ataki na infrastrukturę i sieć

Zabronione jest w szczególności:

a) inicjowanie, organizowanie lub uczestnictwo w atakach typu **DDoS (Distributed Denial of Service)** lub innych atakach odmowy usługi, niezależnie od celu;
b) skanowanie portów, sieci lub systemów bez wyraźnej autoryzacji właściciela docelowego systemu;
c) próby łamania zabezpieczeń (brute-force, exploiting, privilege escalation) wobec infrastruktury Usługodawcy

lub systemów osób trzecich;
d) przechwytywanie ruchu sieciowego (sniffing, MITM) bez wyraźnej autoryzacji;
e) wykorzystywanie Usługi jako **otwartego proxy**, węzła sieci TOR (exit node), VPN tunelu służącego do anonimizacji ruchu osób trzecich — bez uprzedniej pisemnej zgody Usługodawcy.

3.2. Rozsyłanie niechcianych wiadomości (spam)

Zabronione jest w szczególności:

a) rozsyłanie **niezamówionych wiadomości e-mail** (spam) w jakiejkolwiek formie i ilości;
b) wykorzystywanie Usługi do wysyłki wiadomości z fałszywym nagłówkiem nadawcy (spoofing);
c) prowadzenie list mailingowych bez zgody adresatów lub bez możliwości wypisania się;
d) wykorzystywanie skryptów lub narzędzi do masowej wysyłki wiadomości bez nadzoru człowieka.

3.3. Phishing i oszustwa

Zabronione jest w szczególności:

a) tworzenie stron, skryptów lub wiadomości służących do **wyłudzania danych** (phishing, pharming, social engineering);
b) podszywanie się pod Usługodawcę lub inne zaufane podmioty;
c) przechowywanie lub dystrybucja skradzionych danych (baz danych, haseł, numerów kart, danych osobowych).

3.4. Treści bezprawne

Zabronione jest w szczególności:

a) rozpowszechnianie **treści przedstawiających seksualne wykorzystywanie małoletnich** (CSAM) — Usługodawca zgłasza takie przypadki organom ścigania zgodnie z art. 240 Kodeksu karnego;
b) rozpowszechnianie **mowy nienawiści** — treści nawołujących do nienawiści, przemocy lub dyskryminacji na tle rasowym, etnicznym, religijnym, płciowym lub orientacji seksualnej;
c) rozpowszechnianie treści o charakterze **terrorystycznym** — nawołujących do aktów terroru, instrukcji ich przeprowadzania lub gloryfikujących organizacje terrorystyczne;
d) rozpowszechnianie lub udostępnianie **treści chronionych prawem autorskim** bez zgody uprawnionego podmiotu (piractwo), w szczególności nielegalnych kopii gier, pluginów, tekstur, muzyki, oprogramowania;
e) rozpowszechnianie **złośliwego oprogramowania** (malware) — wirusów, trojanów, ransomware, botnetów, cryptominerów;
f) rozpowszechnianie treści naruszających dobra osobiste, w tym wizerunek i prywatność osób trzecich.

3.5. Wykorzystanie zasobów

Zabronione jest w szczególności:

a) **wydobywanie kryptowalut** (mining) bez uprzedniej pisemnej zgody Usługodawcy;
b) uruchamianie procesów destabilizujących infrastrukturę (np. fork-bomb, infinite spawn loops, memory leaks celowe);
c) trwałe przekraczanie limitów zasobów określonych w Specyfikacji technicznej (CPU, RAM, dysk, przepustowość);

d) wykorzystywanie Usługi do celów niezwiązanych z jej przedmiotem (np. jako serwer plików do dystrybucji masowej bez zgody Usługodawcy, seedbox) w sposób obciążający infrastrukturę ponad miarę;
e) uruchamianie serwerów lub usług niebędących serwerami gier (np. serwery WWW produkcyjne, bazy danych produkcyjne, serwery proxy) bez uprzedniej pisemnej zgody Usługodawcy — chyba że wynika to wprost z Specyfikacji technicznej danej Usługi.

3.6. Nadużycia finansowe

Zabronione jest w szczególności:

a) korzystanie ze skradzionych lub nieautoryzowanych instrumentów płatniczych;
b) podawanie fałszywych danych tożsamościowych lub cudzych danych w celu zawarcia umowy;
c) inicjowanie chargebacków bez uzasadnionej podstawy (tj. mimo prawidłowo wykonanej Usługi);
d) wielokrotne zawieranie umów i korzystanie z prawa odstąpienia w celu uzyskania nieodpłatnego dostępu do Usługi (fly-by-night abuse).

4. Bezpieczeństwo i odpowiedzialność Klienta

1. Klient zobowiązuje się do:
   a) zachowania poufności danych logowania do Konta klienta oraz Panelu sterowania serwerem;
   b) stosowania silnych haseł oraz — w miarę możliwości — dwuskładnikowego uwierzytelniania (2FA);
   c) nieudostępniania danych logowania osobom nieupoważnionym;
   d) niezwłocznego powiadomienia Usługodawcy o każdym podejrzeniu nieautoryzowanego dostępu do Konta lub serwera;
   e) regularnego aktualizowania oprogramowania (w tym serwera gry, pluginów, modów) do wersji bezpiecznych;
   f) stosowania narzędzi anty-cheat i anty-exploit, o ile są dostępne dla danego typu serwera.
2. Klient ponosi odpowiedzialność za szkody wynikłe z braku zachowania środków bezpieczeństwa określonych w ust. 1.

5. Procedura egzekwowania

1. W przypadku stwierdzenia lub uzasadnionego podejrzenia naruszenia AUP Usługodawca stosuje procedurę określoną w §10 Regulaminu (zawieszenie Usługi, wezwanie do usunięcia naruszenia, rozwiązanie umowy).
2. Usługodawca klasyfikuje naruszenia wg wagi:
   - **Naruszenia krytyczne** (CSAM, terroryzm, ataki DDoS na infrastrukturę, malware) — natychmiastowe zawieszenie bez uprzedniego wezwania, zgłoszenie do organów;
   - **Naruszenia poważne** (piractwo, phishing, mining bez zgody, spam masowy) — zawieszenie z wezwaniem do usunięcia naruszenia w terminie 24 godzin;
   - **Naruszenia mniejsze** (przekroczenie limitów, brak aktualizacji bezpieczeństwa) — powiadomienie z wezwaniem do usunięcia w terminie 7 dni, ograniczenie zasobów jako środek tymczasowy.
3. Recydywa naruszeń (mniejsze lub poważne) traktowana jest jako naruszenie istotne Regulaminu w rozumieniu §10 ust. 10 Regulaminu.

4. Usługodawca zachowuje prawo do usunięcia lub zablokowania treści bezprawnych bez uprzedniego powiadomienia Klienta, w przypadku gdy wymaga tego prawo (art. 6 Aktu o usługach cyfrowych — DSA, art. 14 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną) lub bezpieczeństwo infrastruktury. Usługodawca przekazuje Klientowi uzasadnienie decyzji zgodnie z §11 Regulaminu niezwłocznie po podjęciu działania.

6. Zgłaszanie naruszeń

1. Każdy może zgłosić podejrzenie naruszenia AUP na adres contact@mchost.gg, podając: identyfikator serwera lub Klienta, opis naruszenia oraz — w miarę możliwości — dowody (logi, zrzuty ekranu).
2. Usługodawca rozpatruje zgłoszenia niezwłocznie, z priorytetem dla naruszeń krytycznych.
3. Zgłaszający zostaje poinformowany o podjętych działaniach, z zastrzeżeniem tajemnicy danych Klienta.

7. Postanowienia końcowe

1. AUP wchodzi w życie z dniem określonym w Regulaminie.
2. W sprawach nieuregulowanych AUP stosuje się Regulamin.
3. AUP jest udostępniane nieodpłatnie w Serwisie w sposób umożliwiający jego pozyskanie, odtwarzanie, utrwalanie i wydrukowanie.