AITY DOCUMENTS

AITY CLOUD SRL

Politica de utilizare acceptabilă

Versiunea 1.0 · în vigoare de la 15 august 2026 · aity.ro/documente

DENUMIRE / ENTITY	AITY CLOUD SRL
CUI	39458128 (RO39458128)
NR. REG. COM.	J2018000824245
EUID	ROONRC.J2018000824245
CORESPONDENȚĂ / CORRESPONDENCE	Str. Heliade Între Vii nr. 35, cod 023382, Sector 2, București, România
CONTACT	office@aity.ro · support@aity.ro · aity.ro · aity.tech

Cuprins

Politica de utilizare acceptabilă

VERSIUNEA 1.0 · ÎN VIGOARE DE LA 15 AUGUST 2026 · AITY CLOUD SRL

English version · Descarcă PDF

Prezenta politică („**AUP**”) face parte din Termenii și condițiile furnizate de **AITY CLOUD SRL**, societate română cu răspundere limitată, cu sediul social în SĂCEL nr. 1003, Sat Săcel, Com. Săcel, MARAMUREȘ, cod 437290, România, CUI 39458128 (RO39458128), înregistrată la Registrul Comerțului sub nr. J2018000824245, EUID ROONRC.J2018000824245, capital social subscris și vărsat 5.000 lei, adresă de corespondență Str. Heliade Între Vii nr. 35, cod 023382, Sector 2, București, România, telefon +40735850896 (luni-vineri, 09:00-18:00, ora României), e-mail office@aity.ro („**aity**”), și se aplică oricărei utilizări a serviciilor aity Platform și aity Cloud. Clientul răspunde de respectarea AUP de către Utilizatorii săi finali. Versiunile în limba română și engleză sunt ambele oficiale; în caz de divergență, versiunea în limba română prevalează.

1. Interdicții generale

Este interzisă utilizarea Serviciilor pentru:

- activități care încalcă legea ori drepturile terților, inclusiv drepturile de proprietate intelectuală, dreptul la viață privată și demnitatea persoanei;
- stocarea sau distribuirea de conținut ilegal, inclusiv materiale care prezintă abuzuri sexuale asupra copiilor (CSAM), conținut care incită la ură sau violență ori care încalcă legislația privind protecția datelor;
- crearea, transmiterea sau distribuirea de malware, ransomware, viruși ori alte componente dăunătoare;
- phishing, înșelăciune, furt de identitate, fraudă ori inducerea în eroare cu privire la originea comunicărilor;
- atacuri informatice de orice fel: acces neautorizat, interceptare, scanare ostilă de porturi, atacuri de tip denial-of-service, ocolirea măsurilor de securitate ale oricărui sistem;
- orice activitate de natură să afecteze securitatea, integritatea sau disponibilitatea infrastructurii aity ori a serviciilor furnizate altor clienți.

2. Reguli specifice e-mailului (aity Platform)

- **Spam interzis**: transmiterea de mesaje comerciale nesolicitate este interzisă. Mesajele comerciale pot fi trimise numai destinatarilor care și-au dat consimțământul prealabil (opt-in) ori în condițiile permise de art. 12 din Legea nr. 506/2004, cu identitate reală a expeditorului, antete corecte și mecanism funcțional de dezabonare, onorat cu promptitudine.
- Limitele de trimitere (număr de mesaje, destinatari, rată) sunt cele publicate în documentația produsului; aity poate limita temporar (throttle) traficul care prezintă tipar de abuz.
- Sunt interzise: colectarea de adrese fără consimțământ, folosirea de liste cumpărate, „snowshoe spamming”, retransmiterea deschisă și falsificarea identității expeditorului (spoofing).

3. Reguli specifice cloud (aity Cloud)

- Minarea de criptomonede este interzisă pe ofertele gratuite și de probă, iar pe resursele plătite este permisă numai în limitele resurselor contractate;
- este interzisă operarea de servicii care facilitează abuzuri: open resolvers, open proxies, servicii de amplificare/reflection utilizabile în atacuri DDoS;
- traficul de date include 4 TB lunar per instanță; consumul care depășește sistematic această limită este supus politicii de utilizare echitabilă: aity poate propune o soluție dedicată sau poate limita traficul excedentar, cu notificare prealabilă;
- Clientul răspunde de securizarea propriilor workload-uri; instanțele compromise care atacă terți pot fi izolate imediat.

4. Alte restricții

Fără acordul scris al aity, este interzis: să revindeți Serviciile ca serviciu propriu; să utilizați conturi partajate între mai multe persoane fizice pentru a eluda tarifarea per utilizator; să folosiți mecanisme automate de creare de conturi; să testați securitatea Serviciilor (teste de penetrare) fără autorizare prealabilă scrisă.

5. Puncte de contact și semnalarea conținutului ilegal (DSA)

5.1. Destinatarii Serviciilor pot contacta aity direct și rapid prin formularul electronic de la aity.ro/documente/semnalare-continut sau la office@aity.ro. Autoritățile folosesc office@aity.ro. Comunicarea este disponibilă în română și engleză și nu se bazează exclusiv pe instrumente automate. Acestea sunt punctele de contact prevăzute de art. 11-12 din Regulamentul (UE) 2022/2065.

5.2. Semnalarea trebuie să permită transmiterea: (a) unei explicații suficient de fundamentate a motivelor pentru care informația este considerată ilegală; (b) locației electronice exacte, inclusiv URL-ul și orice date suplimentare necesare identificării; (c) numelui și adresei de e-mail ale persoanei care semnalează, cu excepția semnalărilor privind infracțiunile prevăzute la art. 3-7 din Directiva 2011/93/UE; și (d) unei declarații de bună-credință privind exactitatea și caracterul complet al informațiilor.

5.3. aity confirmă primirea fără întârzieri nejustificate, analizează semnalarea în timp util, diligent, obiectiv și nearbitrar și comunică decizia și căile de atac. Confirmarea și decizia se transmit la adresa electronică indicată. Dacă sunt folosite mijloace automate pentru detectare, prioritizare ori decizie, acest fapt este comunicat.

5.4. aity nu are o obligație generală de monitorizare a informațiilor găzduite și nu efectuează investigații generale active. O semnalare suficient de precisă poate da naștere cunoașterii efective în sensul legii și va fi tratată conform prezentului articol.

6. Aplicare

6.1. În caz de încălcare a AUP, aity poate, proporțional cu gravitatea: să solicite remedierea în termen de 24 de ore, să limiteze funcționalitatea ori vizibilitatea, să suspende Serviciile sau Conturile afectate, să elimine ori să blocheze accesul la conținutul ilegal, să rezilieze contractul în caz de încălcări grave sau repetate și să sesizeze autoritățile competente. La alegerea măsurii, aity ține seama de gravitate, frecvență, impact, intenție, cooperare și drepturile tuturor persoanelor afectate.

6.2. În cazurile grave (atacuri în desfășurare, conținut vădit ilegal, risc pentru terți ori pentru infrastructură), aity poate acționa imediat, fără notificare prealabilă, informând Clientul de îndată ce este rezonabil posibil.

6.3. Tarifele recurente rămân datorate pe durata suspendării imputabile Clientului, conform Termenilor.

6.4. Motivarea restricțiilor. Cel târziu la impunerea unei măsuri, aity transmite destinatarului afectat, dacă îi cunoaște datele electronice de contact, o motivare clară, specifică și ușor de înțeles care indică: măsura, întinderea teritorială și durata; faptele și împrejurările, inclusiv originea semnalării sau investigației; utilizarea mijloacelor automate; temeiul legal și motivele caracterului ilegal ori clauza contractuală și motivele incompatibilității; și căile disponibile de contestare internă, extrajudiciară și judiciară, după caz. Excepțiile se aplică numai în condițiile art. 17 din Regulamentul (UE) 2022/2065.

6.5. Moderare și contestare. Filtrele anti-spam, anti-malware și mecanismele de securitate pot detecta, prioritiza, pune temporar în carantină ori opri tehnic un atac. O restricție materială a Contului sau încetarea implică analiză umană. Clientul ori destinatarul afectat poate contesta la office@aity.ro, indicând decizia și motivele; o persoană care nu a luat decizia inițială reanalizează cazul, când este practic posibil, și comunică rezultatul pe un suport durabil. Această cale nu limitează mecanismele extrajudiciare sau judiciare disponibile potrivit legii.

6.6. Siguranța persoanelor. Dacă aity ia cunoștință de informații care dau naștere unei suspiciuni privind o infracțiune ce implică o amenințare la adresa vieții sau siguranței unei persoane, notifică prompt autoritățile competente potrivit art. 18 din Regulamentul (UE) 2022/2065 și păstrează evidența deciziei și a informațiilor transmise.

7. Raportarea vulnerabilităților

Vulnerabilitățile care pot afecta Serviciile pot fi raportate confidențial la security@aity.ro, în condițiile politicii publicate la aity.ro/documente/securitate și ale fișierului `/.well-known/security.txt`. Raportul ar trebui să identifice Serviciul, vulnerabilitatea, pașii de reproducere și datele de contact ale raportorului. aity confirmă primirea, protejează raportarea responsabilă efectuată cu bună-credință în limitele politicii și comunică un calendar rezonabil de remediere, fără a solicita accesarea ori divulgarea datelor altor persoane.

Istoricul versiunilor

VERSIUNE	DATA	MODIFICĂRI
1.0	15 august 2026	Prima versiune publicată.