Security Policy for Prime Intellect AI

Updated: May 6, 2026

Scope and Authorization

Prime Intellect AI welcomes security vulnerability reports regarding our public-facing infrastructure, including our website and API endpoints at *.primeintellect.ai. Security researchers must conduct testing in a manner that does not disrupt service availability or compromise customer data integrity.

Vulnerability Reporting Process

To submit a security vulnerability report:

- Send detailed findings ONLY to: security@primeintellect.ai
- Include comprehensive reproduction steps, impact assessment, and supporting evidence
- Adhere to responsible disclosure practices by allowing sufficient remediation time before any public disclosure

IMPORTANT: We only accept and respond to vulnerability reports submitted via email to security@primeintellect.ai. Reports submitted through other channels (including but not limited to Telegram, Discord, social media, or personal email addresses) will not be considered valid submissions and are not eligible for rewards or acknowledgment. For encrypted communications, please use our PGP key available at https://primeintellect.ai/security.

Security Contact Information

Our security contact information and PGP public key for encrypted communications are available at https://primeintellect.ai/security. We encourage researchers to use PGP encryption when sharing sensitive vulnerability details.

Our Commitment

Prime Intellect AI is committed to:

- Acknowledging all reports within 2 business days
- Providing regular status updates throughout the resolution process
- Recognizing contributors for verified submissions (with explicit consent)
- Offering safe harbor protection for good-faith security research conducted within these guidelines

Prohibited Testing Activities

The following activities are expressly prohibited:

- Denial of service (DoS/DDoS) testing or any activity degrading system availability
- Social engineering attacks targeting our employees or users
- Physical security testing of our facilities
- Automated vulnerability scanning without prior written authorization
- Actions that could result in unauthorized access, modification, or destruction of data

Resolution Timeframes

We strive to address security vulnerabilities according to the following timeframes:

- Critical vulnerabilities: 24-48 hours
- High severity issues: 7 business days
- Medium severity issues: 14 business days
- Low severity issues: 30 business days

Vulnerability Rewards

Prime Intellect AI provides compensation for valid security vulnerability reports. Reward amounts are determined based on:

- Severity of the vulnerability
- Quality of the report and reproduction steps
- Potential impact on our systems and users

We evaluate each submission individually. Final reward determinations are at the discretion of our security team.

Eligibility For Rewards

To be eligible for compensation:

- The vulnerability must be previously unknown and verified by our security team
- The report must include sufficient information to reproduce the issue
- The researcher must not have violated any aspects of this security policy
- The vulnerability must represent a genuine security risk

Prime Intellect AI values the security research community’s contributions to maintaining the integrity and security of our systems. Thank you for your commitment to responsible disclosure practices.

Identity Verification And Payment Process

Prime Intellect AI reserves the right to conduct Know Your Customer (KYC) verification for all reward recipients. This process helps us:

- Comply with applicable laws and regulations
- Prevent fraud and ensure proper payment processing
- Maintain compliance with international sanctions and anti-money laundering requirements

To receive payment, you may be required to provide:

- Legal name and address
- Government-issued identification
- Tax information relevant to your jurisdiction
- Other documentation as required by applicable regulations

All personal information collected during this process will be handled in accordance with our Privacy Policy and applicable data protection laws.