Vulnerability Disclosure Policy

Brand Promise

Keeping user information safe and secure is a top priority for us at IPRally Technologies Oy, and we welcome the contribution of external security researchers. We are committed to working collaboratively with the security community to protect our users and maintain the integrity of our services. This Vulnerability Disclosure Policy is designed to encourage responsible security research while protecting both IPRally and our users' data. We appreciate the security community's contributions to keeping our platform secure.

Scope and Targets

In Scope

- **Static marketing site:** IPRally | AI Patent Search, Review & Classification
- **Main web application:** Patent search.
- **Backend APIs:** https://api.iprally.com
- **All subdomains:** *.iprally.com (excluding third-party services listed below)

Out of Scope

- **Third-party hosted** authentication infrastructure managed by external identity providers
- **Physical security** of IPRally facilities
- **Social engineering** attacks (phishing, vishing, smishing)
- **Denial of Service** attacks or load testing
- **Third-party integrations** and services we do not directly control

Research Guidelines

Authorized Activities

- **Security testing** on in-scope targets only
- **Proof-of-concept development** to demonstrate vulnerabilities
- **Minimal data access** necessary to demonstrate impact

Prohibited Activities

- **Accessing, modifying, or deleting** IPRally or customer data
- **Exploiting vulnerabilities** beyond proof-of-concept demonstration
- **Compromising user privacy** or violating data protection laws
- **Disrupting services** or degrading system performance
- **Social engineering** of IPRally employees or customers

Data Protection and Privacy Requirements

In accordance with GDPR and our commitment to data protection:

- **Do not access personal data** - If you inadvertently encounter personally identifiable information (PII), stop immediately and contact us
- **Purge any obtained data** - Delete any accidentally accessed information from your systems
- **Report PII exposure** - Immediately notify us at security-reports@iprally.com if you discover a data exposure
- **Comply with applicable laws** - Ensure your research activities comply with GDPR and other applicable data protection regulations

Excluded Finding Types

The following findings are **not eligible** for our vulnerability disclosure program:

Low Priority/Informational

- Informational findings without demonstrated security impact (stack traces, server errors)
- HTTP 404 or other non-200 response codes
- Banner disclosure on common/public services
- Disclosure of known public files (robots.txt, sitemap.xml)
- Missing security headers without demonstrable exploit path

Authentication/Session Issues

- Account brute force attempts without successful bypass demonstration
- Logout CSRF vulnerabilities
- Password/autocomplete functionality presence

Client-Side Issues

- Self-XSS vulnerabilities
- Clickjacking without exploitable sensitive actions
- CSRF on publicly available forms (contact forms, newsletters)

Cryptographic

- BEAST attack vectors
- SSL/TLS cipher preference issues without practical exploitation

How to Submit a Report

Contact Information

- **Primary contact:** security-reports@iprally.com
- **PGP encryption:** Recommended for sensitive reports
- **PGP Key:** [Contact us for our current public key]

Report Requirements

Please provide:

1. **Clear vulnerability description** and potential impact
2. **Step-by-step reproduction** instructions
3. **Affected systems/URLs** within our scope
4. **Supporting evidence** (screenshots, logs, proof-of-concept)
5. **Your contact information** for follow-up communication

Submission Guidelines

- **One vulnerability per report** - Submit separate reports for distinct issues
- **Detailed documentation** - Include all necessary information for reproduction
- **English language** - All reports should be submitted in English

Response Timeline and Process

We commit to the following response standards:

- **Initial acknowledgment:** Within 5 business days of submission
- **Vulnerability validation:** Within 15 business days
- **Regular updates:** Every 15 business days until resolution
- **Resolution target:** 90 days for validated vulnerabilities
- **Critical issues:** Expedited handling within 30 days

Recognition Program

This Vulnerability Disclosure Program does not provide monetary rewards. However, we recognize and appreciate responsible disclosures through:

Security Researchers Hall of Fame

- **Public recognition** on our website (with your permission)
- **Annual acknowledgment** in our security report
- **LinkedIn recommendations** for significant contributions (upon request)

Professional Recognition

- **Reference letters** for career opportunities (for substantial findings)
- **Conference speaking opportunities** (for major discoveries, jointly presented)
- **Direct communication** with our security team for career networking

Recognition Criteria

- **Valid vulnerability** confirmed by our security team
- **Professional conduct** throughout the disclosure process
- **Compliance** with this policy and applicable laws

Safe Harbor and Legal Protection

IPRally Technologies Oy supports safe harbor for security researchers who:

Good Faith Research

- Make a **good faith effort** to avoid privacy violations and service disruption
- Only interact with **accounts you own** or have explicit permission to test
- **Comply with this policy** and applicable laws throughout your research

Legal Commitments

We will not initiate legal action, refer matters to law enforcement, or pursue civil claims against security researchers who:

- Conduct authorized research under this policy
- Report vulnerabilities through proper channels
- Do not publicly disclose findings before coordinated release unless otherwise agreed in writing or after 90 days

Coordinated Disclosure

Our Commitments

- **Collaborative approach** to disclosure timeline
- **Regular communication** throughout the remediation process

- **Credit and recognition** for your contribution (with your permission)

Disclosure Timeline

- **Standard timeline:** 90 days from validated report
- **Extension requests:** We may request additional time for complex issues
- **Critical vulnerabilities:** Expedited fixes within 30 days
- **Public disclosure:** Only after mutual agreement or timeline completion

Communication and Updates

During Investigation

- **Regular status updates** every 15 business days
- **Technical questions** and clarifications as needed
- **Remediation timeline** discussions

Post-Resolution

- **Disclosure coordination** for public release
- **Technical details** sharing for educational purposes
- **Recognition process** initiation

Contact Information

For vulnerability reports:

- Email: security-reports@iprally.com
- PGP: Request our public key for encrypted communications

For policy questions:

- Email: security@iprally.com
- Reference: "VDP Policy Inquiry" in subject line

Data Controller:

IPRally Technologies Oy
Mikonkatu 15 A
00100 Helsinki, Finland
Business ID: 2901197-7

Policy Updates

This policy may be updated periodically to reflect:

- **Service changes** and new in-scope targets
- **Legal requirements** and regulatory updates

- **Process improvements** based on researcher feedback

Last modified: Feb 17, 2026