Acceptable Usage Policy (AUP)

Version: 1.6
Effective Date: 1st June, 2025
Approved by: Anirudh Loya, CEO
Next Review: 1st June, 2026

1. Purpose

This policy defines the acceptable use of Vrinda Techapps India Pvt Ltd IT resources, ensuring security, compliance, and efficiency. It applies to employees, contractors, and third parties who access company networks, systems, and data.

2. Scope

This policy covers:

- Company-owned devices (laptops, desktops, mobile phones, tablets, servers)
- Network access, internet usage, and VPN connections
- Email, collaboration tools, and messaging platforms
- Cloud services, databases, and software development environments
- Confidential data, including client and proprietary information

3. Acceptable Usage

Employees and authorized users must:

Use IT resources strictly for work-related activities

- Follow security best practices (strong passwords, multi-factor authentication, regular updates)
- Store data in company-approved cloud storage or repositories (e.g., GitHub, AWS, Azure, internal servers)
- Encrypt sensitive data and follow data privacy regulations (e.g., GDPR, HIPAA, CCPA, depending on business operations)
- Follow coding standards, software development policies, and version control protocols

4. Prohibited Activities

Users must NOT:

- Install or use unauthorized software, plugins, or extensions
- Bypass security controls, such as firewalls, VPNs, or access restrictions
- Engage in hacking, penetration testing, or reverse engineering without b company approval
- Share company credentials or allow unauthorized access to company systems
- Store confidential data on personal devices or unapproved third-party platforms
- Engage in excessive personal use of company resources (e.g., social media, streaming)

- Download, distribute, or store illegal, pirated, or inappropriate content
- Use company systems for personal software development projects

5. Security and Data Protection

- Remote Access: Employees must use VPNs and secure connections when working remotely.
- Device Security: All company devices must have endpoint protection, encryption, a regular updates.
- Monitoring: The company may monitor network activity, emails, and device usage to prevent threats.

6. Software Development & Code Management

- Use approved repositories (e.g., GitHub, GitLab, Bitbucket) for code storage
- Do not hardcode sensitive information (e.g., API keys, passwords) in source code
- Follow secure coding practices to prevent vulnerabilities like SQL injection and XSS attacks

7. Consequences of Violations

Any violation of this policy may result in:

- Access restrictions or suspension of IT privileges
- Formal disciplinary action (e.g., written warnings, termination)
- Legal action if violations involve criminal activity, data theft, or intellectual property infringement

8. Acknowledgment & Compliance

All users must acknowledge that they have read, understood, and agree to abide by this Acceptable Usage Policy. The company reserves the right to update the policy as needed.