# ****Information Security Policy:**** Rule of Least Privilege Policy

**Policy Statement:**

The Rule of Least Privilege (RoLP) is a fundamental principle governing access to company systems and data. This policy ensures that individuals are granted the minimum level of access necessary to perform their job functions, minimizing the risk of unauthorized access, data breaches, and other security incidents.

**1. Principle of Least Privilege:**

a. **Access Restriction:** Access rights to information systems and data will be restricted to the minimum necessary for individuals to carry out their job responsibilities.

b. **Default Deny:** Unless specifically authorized, access to systems, applications, and data is denied by default.

**2. User Account Management:**

a. **Access Approval Process:** Access requests must be submitted through an official approval process and granted based on job roles and responsibilities.

b. **Periodic Review:** Regularly review and update user access rights to ensure alignment with current job functions.

**3. No Local Admin Privileges:**

a. **Prohibition:** Local administrative privileges on workstations and servers are strictly prohibited.

b. **Exception Handling:** Any exceptions to this policy must be approved by the IT department and documented with a clear justification for the elevated privileges.

**4. Remote Access:**

a. **Minimum Necessary Access:** Remote access privileges will be granted based on the minimum level necessary for individuals to perform their duties.

b. **Secure Authentication:** Implement secure authentication methods for remote access, such as multi-factor authentication (MFA).

**5. Temporary Privileges:**

a. **Limited Duration:** Temporary elevated privileges may be granted for specific tasks and must be revoked immediately upon completion.

b. **Documentation:** Maintain documentation for all instances of temporary privilege elevation, including the reason and duration.

**6. Monitoring and Auditing:**

a. **Access Logs:** Regularly review access logs to monitor user activities and identify any unauthorized or suspicious access.

b. **Periodic Audits:** Conduct periodic audits to ensure compliance with the Rule of Least Privilege.

**7. Training and Awareness:**

a. **User Training:** Provide regular training to employees on the principles of least privilege and the importance of secure access practices.

b. **Communication:** Communicate policy updates and reminders to all users to reinforce the importance of adhering to the Rule of Least Privilege.

**8. Policy Enforcement:**

a. **Consequences of Violation:** Violation of this policy may result in disciplinary actions, including but not limited to access restrictions, suspension, or termination.

b. **Reporting Violations:** Employees are encouraged to report any suspected violations of this policy promptly.

**9. Policy Review:**

This policy will be subject to periodic review and updates to align with industry best practices and emerging cybersecurity threats.

**Acknowledgment:**

By accessing company systems and services, users acknowledge their understanding of and commitment to complying with this Rule of Least Privilege Policy.

*Date of Policy Implementation: (DATE)*

*Policy Owner: (COMPANY NAME)*