Risk Acceptance and Tolerance Justification

1. Document Information

Document ID: RA-2024-001

Date: 2024-06-10

Prepared by: Jane Doe, Information Security Officer

Department: IT Security

2. Risk Description

Risk Title: Insecure Web Application Authentication
Risk Statement: The current web application utilizes outdated authentication mechanisms, which may be susceptible to brute-force and credential-stuffing attacks due to lack of multi-factor authentication.

3. Risk Assessment Summary

- **Likelihood:** Medium
- **Impact:** High
- **Risk Rating:** Significant
- **Existing Controls:** Web firewall, strong password policy, regular user awareness training.

4. Justification for Acceptance/Tolerance

Although the risk is significant, critical mitigating controls are currently in place. Implementation of multi-factor authentication is scheduled within the next six months as part of the IT security roadmap. The cost and operational impact of immediate remediation are currently prohibitive relative to the risk exposure. Stakeholders have agreed to tolerate the current risk level for this interim period.

5. Review & Approval

Risk Owner: John Smith, Head of IT
Approval Date: 2024-06-09
Review Date: 2024-12-09

Important Notes:

- Risk acceptance must be formally reviewed and documented with clear justification.
- Periodic re-evaluation is essential to ensure continued relevance and appropriateness.
- Stakeholders should be aware of and agree to any accepted or tolerated risks.
- This document is subject to audit and compliance verification.
- Contingent plans should be in place for escalation if risk conditions change.