Request for Change (RFC)

Change Title

Transition from Password-Based Authentication to Passwordless Authentication

Change Request ID

RFC-2026-001

Requested By

IT Security Team

Date

January 2026

---

1. Description of the Desired Change

This RFC proposes transitioning the organization's user authentication mechanism from traditional password-based authentication to **passwordless authentication methods**, specifically biometric authentication such as **fingerprint scanning** and **facial recognition**, where supported.

Passwordless authentication would be implemented using supported operating system features and identity platforms (e.g., Windows Hello, mobile device biometrics, or identity provider-based biometric authentication). Passwords would be reduced or eliminated for routine user logins, while remaining available for fallback or administrative access where required.

The goal of this change is to improve security, reduce credential-based attacks, and enhance the user authentication experience.

---

2. Expected Impact on the Business

Positive Impacts:

- **Improved security posture** by reducing exposure to phishing, password reuse, brute-force attacks, and credential stuffing.
- **Reduced help desk workload** due to fewer password reset requests.

- **Improved user experience** through faster and simpler authentication.
- **Alignment with modern security best practices** and zero-trust principles.

Potential Negative Impacts:

- Initial **user training and adjustment period**.
- Possible **hardware compatibility issues** for systems lacking biometric capabilities.
- Temporary productivity impact during rollout and enrollment phases.

Overall, the change is expected to provide long-term operational and security benefits that outweigh short-term disruption.

---

3. Risk Assessment

Identified Risks:

- **Biometric enrollment failures** or false rejections impacting user access.
- **Privacy concerns** related to biometric data handling.
- **Device compatibility limitations** for older hardware.
- **System integration issues** with legacy applications.

Risk Mitigation Measures:

- Use biometric systems that store data securely on-device (not centrally stored).
- Maintain fallback authentication methods (PINs or passwords).
- Pilot the change with a limited user group before full deployment.
- Provide clear user guidance and support during enrollment.

---

4. Rollback Plan

If the change fails or causes unacceptable disruption, the following rollback plan will be enacted:

1. Disable biometric authentication requirements.
2. Re-enable password-based authentication across all affected systems.
3. Notify users of the rollback and provide guidance for resuming password use.

4. Review logs and incident reports to identify root causes.
5. Revise the implementation approach before any future reattempt.

Rollback procedures will be documented and tested prior to implementation.

---

5. Individuals / Groups Involved

- **IT Security Team** – Change ownership, security validation
- **IT Infrastructure Team** – System configuration and deployment
- **Help Desk / Support Team** – User support and issue resolution
- **End Users** – Enrollment and authentication usage
- **Management / Change Advisory Board (CAB)** – Review and approval

---

6. Proposed Implementation Schedule

Phase	**Description**	**Timeline**
Planning & Approval	RFC review and approval	Week 1
Pilot Deployment	Limited user group testing	Weeks 2–3
User Training	Documentation and guidance	Week 3
Full Deployment	Organization-wide rollout	Weeks 4–5
Post-Implementation Review	Validate success and address issues	Week 6

---

7. Systems and Services Affected

- User workstations and laptops
- Mobile devices used for corporate access
- Identity and access management (IAM) systems
- Operating system authentication services
- VPN and remote access services

- Internal applications integrated with centralized authentication

---

Approval

- **Change Manager:** ________________________
- **Date:** ________________________