# API Token Storage Protocol

Purpose:

To ensure secure handling and storage of Freshservice API tokens used in workflow automation and external integrations.

Best Practices:

**1. Use Environment Variables**

* Store tokens in secure server-side environment variables.
* Avoid hardcoding tokens in scripts or workflow payloads.

**2. Restrict Token Scope**

* Generate tokens with the least privilege required.
* Use separate tokens for each integration to improve auditing.

**3. Rotate Tokens Regularly**

* Establish a quarterly token rotation schedule.
* Document token expiration dates and owners.

**4. Audit Usage**

* Monitor access logs for token misuse or anomalies.
* Revoke tokens no longer in use.

**5. Encrypt At Rest and In Transit**

* If storing tokens temporarily, encrypt using AES-256 or similar.
* Ensure HTTPS is always used for webhook communication.

**6. Use Secrets Management Tools**

* Tools such as HashiCorp Vault, AWS Secrets Manager, or Azure Key Vault are recommended for production systems.

**7. Avoid Sharing Over Email/Chat**

* Tokens should never be shared over unencrypted channels or stored in shared documents.

Enforcement:

All integrations using Freshservice API tokens must conform to this protocol and undergo periodic review.

Owner: Automation & Integration Lead

Effective Date: 2025-01-01