Freshservice – API Token Storage Protocol (for Automation Security)

This document outlines the security protocol for storing and managing API tokens used in automation within Freshservice. The protocol aligns with ITIL practices in Information Security Management, Service Automation, and Configuration Management.

# 1. Purpose

To establish a secure and auditable method for managing Freshservice API tokens used in integrations and automation scripts. This ensures compliance with access control, audit readiness, and ITIL-aligned security governance.

# 2. Scope

This protocol applies to all Freshservice automation initiatives, including webhooks, workflow automator scripts, external integrations, and scheduled jobs that use API authentication tokens.

# 3. Token Generation Guidelines

- Tokens must be generated using a dedicated Freshservice account with least-privilege access  
- Assign tokens per use-case (e.g., provisioning, notifications, 3rd-party integrations)  
- Log the purpose and configuration of each token

# 4. Secure Storage Recommendations

- Store API tokens in enterprise-grade secrets managers (e.g., AWS Secrets Manager, Azure Key Vault, HashiCorp Vault)  
- Do not store tokens in plain text files, spreadsheets, or unsecured script headers  
- Automate token injection into CI/CD pipelines or integration jobs

# 5. Access Control & Auditability

- Token vault access must be restricted using role-based access control (RBAC)  
- Logs should capture token access, update, and deletion events  
- Conduct periodic reviews of access permissions per ITIL audit policies

# 6. Token Expiry and Rotation

- Where supported, set expiration dates on tokens and establish renewal intervals  
- Implement alerts for upcoming token expiries  
- Rotate tokens every 90 days or as defined by your organizational policy

# 7. Emergency Procedures

- In case of token leakage or exposure, revoke affected tokens immediately  
- Perform root cause analysis and notify affected systems/users  
- Document the incident as part of an ITIL security incident report

# 8. Documentation and CMDB Integration

- Register all automation tokens in the Configuration Management Database (CMDB)  
- Track which systems and workflows depend on each token  
- Tag tokens with service association and owner information