# My Big Company Operations Manual

## 1. Introduction

### 1.1 Purpose

This document outlines the operational procedures, maintenance guidelines, and governance structure for My Big Company’s Ansible Automation Platform (AAP) infrastructure.

### 1.2 Scope

This manual applies to all automation operations within Server Engineering and Operations, including job execution, security policies, access management, and compliance.

### 1.3 Audience

* **Platform Engineers** – Responsible for maintaining and optimizing automation workflows.
* **Platform Operators** – Execute automation workflows as per the defined policies.
* **Platform Administrators** – Manage access control, execution policies, and troubleshooting.
* **Security & Compliance Teams** – Ensure adherence to compliance standards.

## 2. Platform Overview

### 2.1 Environment & Infrastructure

* **Environment Type**: On-Prem
* **Primary Objectives**: [‘Automation’, ‘SRE’, ‘DevSecOps transformation’, ‘Cost optimization’]
* **Supported OS Versions**:
  + **RHEL**: 8, 9
  + **Windows**: 2016, 2019, 2022
* **Ansible Automation Platform Version**: 2.5
* **Red Hat Satellite Version**: 6.13

### 2.2 Infrastructure Components

* **Identity Management System**: Active Directory, Okta
* **RBAC Provider**: SailPoint, FreeIPA
* **Load Balancer**: F5 Big-IP
* **Inventory Management**: Red Hat Satellite, Ansible Inventory
* **Credential Storage**: CyberArk, HashiCorp Vault

## 3. Operational Procedures

### 3.1 Job Execution Policies

* **Policy**: Restricted to approved job templates
* Only approved job templates are executed.
* Jobs are logged and audited for compliance.

### 3.2 Maintenance Schedule

* **Routine Maintenance**: Every Quarterly.
* **Patching**: Managed through Red Hat Satellite, Ansible Inventory.

### 3.3 Security & Compliance

* **Compliance Standards**: CIS Level 1, RBAC, SailPoint
* **Audit Frequency**: Quarterly
* **Monitoring & Logging**: Splunk, BMC Helix, Red Hat Satellite

## 4. Technology Stack

### 4.1 Infrastructure

* **Network Technologies**: Cisco Fabric, Infoblox (DNS)
* **Security Technologies**: Tenable, SentinelOne, Splunk
* **Compute Technologies**: VMware vSphere, Red Hat OpenShift

### 4.2 Configuration & Deployment

* **Configuration Management**: Ansible Automation Platform, GitLab
* **Storage Systems**: Pure Storage, Dell EMC
* **Identity & Access Management**: Okta, Active Directory, SailPoint

### 4.3 Monitoring & Logging

* **Service Management Tools**: BMC Helix, Digital Workplace
* **Containerization Platforms**: Red Hat OpenShift, Docker
* **Application Management**: MuleSoft, Archer

## 5. Performance Metrics & Governance

### 5.1 Key Metrics

Performance of AAP is tracked using the following key metrics: - **Automation Coverage**: Automation Coverage (%), Change Lead Time, Incident MTTR, Configuration Drift (%)

### 5.2 Governance Model

* **Role-Based Access Control (RBAC)** is enforced via SailPoint, FreeIPA.
* **Platform Admins** manage high-level configuration and access.
* **Operators** are limited to executing approved job templates.

### 5.3 Approval Workflow

* **Changes impacting security, compliance, or architecture require approval from the Principal Engineer.**
* **Minor updates can be approved by Platform Engineers or Administrators.**

## 6. Roles & Responsibilities

|  |  |  |
| --- | --- | --- |
| Role | Responsibilities | Decision Authority |
| **Principal Engineer** | Define governance, approve procedures, ensure compliance. | Final authority on governance & security. |
| **AAP Engineer** | Implement configurations, troubleshoot job execution issues. | Executes within defined governance. |
| **Platform Administrator** | Manage platform-wide settings, user access, and security. | Admin control over infrastructure. |
| **Platform Operator** | Execute approved workflows, report issues. | Limited execution authority. |
| **Platform Auditor** | Monitor compliance, review security adherence. | Read-only audit access. |

## 7. Change Management & Audit

### 7.1 Change Control Process

* All modifications follow a structured **change request** process.
* Requests are reviewed based on their impact on:
  + **Security**
  + **Compliance**
  + **Operational Stability**

### 7.2 Compliance Auditing

* **Audit Schedule**: Quarterly.
* **Audited By**: SailPoint, FreeIPA security teams.
* **Logged & Monitored By**: Splunk, BMC Helix, Red Hat Satellite.