

Automated Provisioning Plan

Enterprise Hub Network Infrastructure

Prepared by: Alpha Team

Date: October 2025

1. Executive Summary

This plan automates the provisioning of a secure, segmented cloud network reflecting the provided enterprise topology. Each department is mapped to a subnet with Transit Gateway hub-and-spoke routing, hybrid VPN connectivity, and guardrails.

2. Objectives

- Provision VPC and departmental subnets with Transit Gateway in <30 minutes.
- Ensure >95% idempotent Terraform applies.
- Enforce policy-as-code with tagging and encryption standards.
- Enable hybrid Site-to-Site VPN for printers and legacy servers.

3. Scope

In-scope components include AWS VPC, subnets, TGW, route tables, IAM roles, EC2 base images, monitoring, logging, and KMS encryption. Out-of-scope items include application deployment, data migration, and on-prem printer configuration.

4. Security & Compliance

Security is ensured through IAM least privilege, private subnets, NAT gateways, encryption at rest and in transit, and auditing via CloudTrail and Config. Compliance is enforced by mandatory tagging and OPA checks.

5. Change Management

All infrastructure changes follow GitOps workflows: feature branches → PR → plan review → approval → apply. Rollback strategy is forward-fix or controlled resource replacement, with logs and state backups retained.