Aventex Inc. Security program

This document establishes the **Physical and CyberSecurity Program** for Aventex Inc.

1. Purpose

The purpose of this program is to mitigate internal and external risks. It ensures our customers and partners that Aventex meets high standards of integrity and reliability. This policy protects Aventex Inc. assets, client data, and proprietary systems.

2. Scope

This policy applies to all personnel at Aventex Inc. This includes full-time employees, part-time employees, interns, contractors, and external consultants operating out of the 25505 Kensington Place, Great Neck, NY office or working remotely.

3. Identity and Access Management (IAM)

- **Central Identity Provider:** All employee access goes through a central directory
- **Mandatory MFA:** Multi-factor authentication is strictly enforced on all cloud accounts. Phishing-resistant options (like security keys or passkeys) are preferred.
- **Single Sign-On (SSO):** Staff must use company SSO to log into SaaS applications. This ensures immediate access revocation during offboarding.
- **Role-Based Access Control (RBAC):** Access to cloud environments (AWS, Azure, Google Cloud) is assigned based on job roles, never granted globally. [1]

2. Cloud Infrastructure and SaaS Security

- **No Local Hosting:** No production data, client databases, or applications are hosted on premises at the Great Neck office.
- **Configuration Audits:** Cloud environments are audited quarterly using automated tools to detect misconfigured storage buckets or open ports. [1, 2]
- **Data Loss Prevention (DLP):** Sharing controls are enforced in cloud storage to prevent confidential documents from being shared publicly or with personal email accounts. [1]

3. Endpoint and Remote Work Security

- **Zero Trust Network Access (ZTNA):** Traditional office firewalls are replaced by a Zero Trust model. Access to data depends on device health and user identity, not physical location.
- **MDM Enforcement:** All corporate laptops must be enrolled in Mobile Device Management (MDM). Non-enrolled personal devices are blocked from cloud tools.
- **Public Wi-Fi Policy:** Employees working outside the Great Neck office must use an approved secure network or an encrypted corporate VPN.

---

4. Workplace Access Control

- **Purpose:** The Great Neck facility protects personnel and corporate hardware (laptops), not data centers.
- **Locked Entry:** The office suite door at 25505 Kensington Place must remain locked at all times. Employees gain entry via digital keys or fobs.
- **Visitor Policy:** Clients and guests must register at reception, be escorted by staff, and remain in public meeting spaces.

5. Asset Protection and Office Monitoring

- **Clean Desk and Screen Policy:** Employees must lock their laptop screens (Win + L or Cmd + Ctrl + Q) every time they walk away from their desks.
- **Local Storage Prohibition:** No corporate or client data may be printed or stored on local external hard drives left in the office.
- **Environmental Security:** The office uses a commercial alarm system and smart cameras covering the main entrances to track after-hours access.