**Remote Access Policy for (AGENCY NAME)**

**1. Purpose**

This section outlines procedures for remote access to (AGENCY NAME)’s systems and network resources. It aims to ensure secure, authorized, and compliant access while protecting sensitive information and maintaining operational efficiency.

**2. Scope**

This policy applies to all personnel, third-party IT support, contractors, and vendors who require remote access to the (AGENCY NAME) network and systems.

**3. Remote Access Definition**

Remote access refers to connecting to the (AGENCY NAME) systems or network through external networks such as the internet. This may include secure remote access methods like (Approved Remote access software), VPN, broadband, or wireless connections.

**4. Approved Remote Access Software**

**5. Remote Access Authorization**

* **Client Initiation**: Users must initiate the remote connection.
* **Access Authorization**: Access is granted only after the completion of mandatory training, which includes:
  + Handling protected information.
  + Proper use of system resources.
  + Compliance with CJIS 5.9.3 and other relevant regulations for law enforcement data.
* **Training**: All users requesting remote access must complete training to ensure compliance with CJIS and other regulations related to protected information.

**6. Authentication & Security**

* **Multi-Factor Authentication (MFA)**: Required for all remote access users, facilitated via the (Approved Remote access software) platform.
* **Encryption Standards**: All remote access connections must use FIPS 140-2 certified encryption.

**7. Session Management & Termination**

* **Time-Out Settings**: Remote sessions will automatically lock or disconnect after 15 minutes of inactivity, requiring re-authentication to resume.
* **Concurrent Sessions**: Limitations on the number of simultaneous remote sessions per user, and session durations will be monitored to prevent unauthorized access.
* **Automatic Session Termination**: Remote access sessions may be terminated due to inactivity, policy violations, or completion of support tasks.

**8. Monitoring and Control**

* **Audit Logs**: All remote access activities will be logged, including login times, session duration, and systems accessed, to detect potential security issues or violations.
* **Security Monitoring**: Continuous monitoring of remote access methods to detect and prevent unauthorized access, attacks, or misuse.

**9. Remote Support Procedure Example**

1. **Client Request**: User contacts support for remote assistance.
2. **Support Login**: Support staff logs in to (Approved Remote access software) with unique credentials.
3. **Multi-Factor Authentication (MFA)**: Support staff authenticates using MFA.
4. **Session Initiation**: Support staff generates a session code, valid for 5 minutes, which the client uses to initiate the session.
5. **Code Entry**: Client enters the code in (Approved Remote access software), automatically downloading the agent for the session.
6. **Encryption**: The remote session is established using (ENCRYPTION PROCESS) for encryption, ensuring secure communication as certified under (FIPS Certification)
7. **Permission Request**: Support staff asks for client permission to view and control their system.
8. **Assistance**: Support staff provides troubleshooting assistance and resolves issues.

**10. Enforcement**

Failure to comply with this policy may result in disciplinary action, including termination, depending on the violation's severity. All remote access activities will be monitored and logged for compliance.