Unique Identifier Policy Sample

(Sample written policy to assist with compliance)

1.0 Purpose

The purpose of this policy is to ensure accountability of all users that access [agency name] networks and network devices.

2.0 Scope

The scope of this policy is to define the creation of a unique identifier for individuals that access <Agency Name> networks, network devices and all equipment that processes, stores, and/or transmits LEIN-based Criminal Justice Information (CJI) and classified and sensitive data that is owned or leased by [agency name].

3.0 Policy

3.1 General

[Agency name] requires that each employee with access to [agency name] networks, applications, and/or LEIN/NCIC for the purpose of storing, processing, and/or transmitting CJI shall be uniquely identified by use of a unique identifier. A unique identifier shall also be required for all persons who administer and maintain the system(s) that access agency and LEIN-based CJI and/or networks. [Agency name] requires users to identify themselves uniquely before the user is allowed to perform any action on the network and/or applications. All user IDs shall belong to currently authorized users. Identification data shall be kept current by adding new users and disabling former users. Employees shall not share their IDs with other employees, supervisors, management, or family members at any time.

3.2 Guidelines

The unique identification can take the form of the following examples:

- User's full name (JohnWDoe)
- Form of full name (SASmith)
- Badge number (WV724966)
- Combination of name and badge number (jhardWV966)
- Serial Number (123456789)
- Other unique alphanumeric identifier

4.0 Penalties

Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, and termination of employment.