<Organization Name>	Information Security Identification and Authentication Policy	
Department Name	Policy #	**Issue Date:** September 13, 2013
Approved by:		

1. Purpose

<Organization Name> <Insert Organization Mission Here>. This policy establishes the Enterprise Identification and Authentication Policy, for managing risks from user access (organizational, non-organizational) and authentication into company information assets through the establishment of an effective identification and authentication program. The identification and authentication program helps <Organization Name> implement security best practices with regard to identification and authentication into company information assets.

2. Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by <Organization Name>. Any information, not specifically identified as the property of other parties, that is transmitted or stored on <Organization Name> IT resources (including e-mail, messages and files) is the property of <Organization Name>. All users (<Organization Name> employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3. Intent

The <Organization Name> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish an identification and authentication capability throughout <Organization Name> and its business units to help implement security best practices with regard to identification and authentication into company information assets.

4. Policy

<Organization Name> has chosen to adopt the Identification and Authentication principles established in NIST SP 800-53 "Identification and Authentication," Control Family guidelines, as the official policy for this domain. The following subsections outline the Identification and Authentication standards that constitute <Organization Name> policy. Each <Organization Name> Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

- IA-1 Identification and Authentication Policy and Procedures: All <Organization Name> Business Systems must develop, adopt or adhere to a formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- IA-2 Identification and Authentication (Organizational User): All <Organization Name> Business Systems must require that organizational users uniquely identify and authenticate into company information assets. Authentication of user identities is

accomplished through the use of password, tokens, biometrics, multi-factor authentication, or some combination thereof.

- IA-3 Device Identification and Authentication: All <Organization Name> Business Systems must require that system devices uniquely identify and authenticate organizational users prior to the establishment of a connection. These mechanisms include but are not limited to Media Access Control (MAC), IEE 802.1x and Extensible Authentication Protocol (EAP), Radius server with EAP-Transport layer Security (TLS) authentication, and Kerberos.
- IA-4 Identifier Management: All <Organization Name> Business Systems must manage information asset identifiers for user and devices by:
    - Receiving authorization from a designated organizational official to assign a user or device identifier.
    - Selecting an identifier that uniquely identifies an individual or device.
    - Assigning the user identifier to the intended party or the device identifier to the intended device.
    - Preventing reuse of user or device identifiers for the period to which it is assigned to an active user or device.
    - Disabling the user identifier after **45 days of inactivity**.
- IA-5 Authenticator Management: All <Organization Name> Business Systems must manage information asset authenticators for users and devices by:
    - Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator.
    - Establishing initial authenticator content for authenticators defined by the organization.
    - Ensuring that authenticators have sufficient strength of mechanism for their intended use.
    - Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
    - Changing default content of authenticators upon information asset installation.
    - Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators where appropriate (i.e., passwords).
    - Changing/refreshing authenticators when appropriate (e.g., passwords, tokens).
    - Protecting authenticator content from unauthorized disclosure and modification.
    - Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

- IA-6 Authenticator Feedback: All <Organization Name> Business Systems must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
- IA-7 Cryptographic Module Authentication: All <Organization Name> Business Systems containing information assets with cryptographic authentication modules must meet the requirements of applicable federal laws, directives, policies, regulations, standards, and guidance for such authentication.
- IA-8 Identification and Authentication (Non-Organizational Users): All <Organization Name> Business Systems must require that non-organizational users uniquely identify and authenticate into company information assets. Authentication of user identities is accomplished through the use of password, tokens, biometrics, multi-factor authentication, or some combination thereof.

Appendix A – References

The following references illustrate public laws which have been issued on the subject of information security and should be used to demonstrate <Organization Name> responsibilities associated with protection of its information assets.

a. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Recommended Security Controls for Federal Information Systems Revision 3, Technical Controls, Identification and Authentication Control Family, August 2009.

b. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-73 “Interfaces for Personal Identity Verification” Revision 3 February 2010.

c. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-63 “Electronic Authentication Guideline” December 2008.

d. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-76 “Biometric Data Specification of Personal Identity Verification” Revision 1 January 2007.

e. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-78 “Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)” Revision 2 February 2010.

f. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 “Information Security Handbook: A Guide for Manager” October 2006.