




Information Technology Identification and Authentication Policy

February 28, 2023



Prepared by:
David Oluyitan,
Information Assurance Lead

Approval

This policy is approved and issued under the authority granted to the Chief Information Officer in accordance with the IT Executive Steering Committee (ESC) Charter.

Dennis Lauer

DENNIS LAUER
Chief Information Officer

February 28, 2023

Date

Identification and Authentication Policy

1. Purpose

The Cadmus Group (Cadmus) Identification and Authentication policy is designed to track all actions within Cadmus network to a single authorized individual, where feasible. While generic account usage is at times inevitable, it must be minimized to only those instances when an individual account cannot be used to accomplish that specific task. Each user is assigned a unique username for access to Cadmus information systems.

2. Scope

This policy applies to:

All employees, contractors, and consultants who maintain network credentials and have access to Cadmus information systems and networks. This includes employees and contractors from The Cadmus Group, Obsidian Analysis, LLC, Cadmus International LLC., and Meister Consulting Group. (Cadmus)

3. Dissemination

This policy is available only to designated individuals within Cadmus with a need-to-know on the internal SharePoint site. The policy is specifically disseminated to members of the following teams: Client Services (CS), Engineering & Operations (ENO), Architecture & Systems Design (ASD), Information Assurance, and Chief Information Officer (CIO).

4. Identification and Authentication (Organizational Users) [NIST SP 800-53, IA-2]

All Cadmus information systems are configured to uniquely identify and authenticate organizational users, where feasible.

(1) Network Access to Privileged Accounts [NIST SP 800-53, IA-2(1)]

- a. Cadmus information systems are configured to implement multifactor authentication in accordance with the assurance level for network access to privileged accounts.

(2) Network Access to Non-Privileged Accounts [NIST SP 800-53, IA-2(2)]

- a. Cadmus information systems are configured to implement multifactor authentication in accordance with the assurance level for network access to non-privileged accounts.

(8) Access to Accounts – Replay Resistant [NIST SP 800-53, IA-2(8)]

Cadmus information systems are configured to use replay-resistant authentication protocols for access to privileged accounts. Techniques used to address this may include protocols

that use challenges (e.g., Transport Layer Security TLS) and time synchronous or challenge-response onetime authenticators.

(11) Remote Access – Separate Device [NIST SP 800-53, IA-2(11)]

Cadmus information systems are configured to implement multifactor authentication in accordance with the assurance level for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets NIST standards.

5. Device Identification and Authentication [NIST SP 800-53, IA-3]

- a) Cadmus information systems are configured to uniquely identify and authenticate end user-operated devices (e.g., workstations, laptops, voice-over-Internet Protocol (VoIP) phones, mobile phones) and servers before establishing a network connection.

6. Identifier Management [NIST SP 800-53, IA-4]

Cadmus information systems:

- a) Receive authorization from a designated Firm official (e.g., project manager, system administrator, or system owner) prior to assigning an individual, group, role, or device identifier.
- b) Select and assign information system identifiers that uniquely identify an individual, group, role, or device, where feasible.
- c) Ensure that no two (2) users or devices have the same identifier.
- d) Disable the identifier after ninety (90) days of inactivity.

7. Authenticator Management [NIST SP 800-53, IA-5]

Cadmus information systems:

- a) Verify the identity of the individual, group, role, or device receiving an information system authenticator as part of the initial authenticator distribution.
- b) Establish unique initial authenticator content for information system authenticators.
- c) Ensure that authenticators have sufficient strength of mechanism for their intended use.
- d) Change default settings of authenticators prior to information system installation.
- e) Adhere to following maximum and minimum lifetime restrictions and re-use conditions regarding authenticators:
 - Passwords have a minimum lifetime of one (1) day and maximum lifetime set to 'never expire.'
 - Password reuse for a specific account is prohibited for 10 generations.
- f) Protect authenticator settings from unauthorized disclosure and modification.
- g) Users maintain possession of their individual authenticators, not loan or share authenticators with others, and report lost or compromised authenticators immediately to their supervisor and IT Client Services (Help Desk).
- h) Change authenticators for shared group/role accounts when membership to those accounts change.

(1) Password-Based Authentication [NIST SP 800-53, IA-5(1)]

Cadmus information systems:

- a. Minimum password complexity:
 1. Password is at least ten (10) non-blank characters long.
 2. All passwords, including initial passwords, is composed of a minimum of one (1) character from at least three (3) of the following four (4) categories:
 - English uppercase characters (e.g., A-Z)
 - English lowercase letters (e.g., a-z)
 - Non-Alphanumeric special characters (e.g., ! @, #, \$, %, ^, &, etc.)
 - Base 10 Digits/Numerals (e.g., 0-9)
- b. At least one (1) character is changed when new passwords are created.
- c. Store and transmit only encrypted representations of passwords.
- d. Enforce passwords minimum lifetime of one (1) day and maximum lifetime set to 'never expire.'
- e. Prohibit password reuse for five (5) generations.
- f. Allow the use of a temporary password for system logins with subsequent notification to user to change to a standard compliant password.

(2) Public Key Infrastructure-Based Authentication [NIST SP 800-53, IA-5(2)]

Cadmus information systems enforce the following for PKI-based authentication on applicable information systems:

- a. Validate certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.
- b. Enforce authorized access to the corresponding private key.

8. Authenticator Feedback [NIST SP 800-53, IA-6]

Cadmus information systems are configured to obscure feedback (e.g., display asterisks when users type passwords into input devices) of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

9. Cryptographic Module Authentication [NIST SP 800-53, IA-7]

Cadmus information systems implement mechanisms for authentication to a cryptographic module that meets the Federal Information Processing Standard (FIPS) 140-2 and guidance for such authentication.

10. Re-Authentication [NIST SP 800-53, IA-11]

Cadmus privileged account users re-authenticate when circumstances or situations require re-authentication during the following:

- a) authenticators or roles change.
- b) security categories of systems change.
- c) the execution of privileged functions occurs.

APPENDIX A: GLOSSARY

Critical Systems – Systems that enable essential business functions and must be monitored, secured from attack, and maintain a high degree of integrity, availability, and confidentiality to prevent disruption in support of Cadmus business operations.

Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems. (Source: NIST, SP 800-53, Revision 4)

Least Privilege – The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. (Source: CNSS, CNSSI 4009)

Multifactor Authentication – Authentication using two or more factors to achieve authentication. Factors include: (1) something you know (e.g. password or personal identification number (PIN)); (2) something you have (e.g., cryptographic identification device, token); or (3) something you are (e.g., biometric). (Source: NIST, NISTIR 7298, Revision 2)

Network Access – Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). (Source: NIST, SP 800-53, Revision 4)

Public Key Infrastructure (PKI) Based Authentication - Public key cryptography is a valid authentication mechanism for individuals and machines or devices. When PKI is implemented, status information for certification paths includes certificate revocation lists or certificate status protocol responses. (Source: NIST, SP 800-53, Revision 5)

Privileged Account – An information system account with authorizations of a privileged user. (Source: NIST, SP 800-53, Revision 4)

Replay Resistant Authentication – Authentication processes resist replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.

System Security Plan (SSP) – Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. (Source: NIST, NISTIR 7298, Revision 2)

The Federal Information Processing Standard (FIPS) 140-2 – An information technology security accreditation program for validating that the cryptographic modules produced by private sector companies meet well-defined security standards.

Cadmus – All employees, contractors, and consultants who maintain network credentials and have access to Cadmus information systems and networks. This includes employees and contractors from The Cadmus Group, Obsidian Analysis, LLC, Cadmus International LLC., Meister Consulting Group.

User – Individual, or (system) process acting on behalf of an individual, authorized to access an information system. (Source: NIST, SP 800-53, Revision 4)

User Account – A mechanism that provides a single individual with access rights and privileges to an information system. Upon authenticating to a user account, a person (the user) is uniquely identified to an information system and is granted the access rights and privileges assigned to that specific account.

RECORD OF CHANGES

This section documents the changes made to Cadmus Information Technology (IT) Identification and Authentication policy.

Version	Date	Author	Description of Changes
0.1	12/19/2019	Matt Pierce	Initial draft
0.2	11/16/2020	David Oluyitan, John O’Keeffe , Ahmed Rafeq, Erik Stillman, Dustin Hermann	IT Policy Updates for 2020 Workshop Session I
0.3	11/18/2020	Oluyitan, O’Keeffe, Hermann	IT Policy Updates for 2020 Workshop Session II
1.0	12/9/2020	Dennis Lauer	Final review and approval
1.1	2/1/2022	David Oluyitan, Erik Stillman	Annual review and update
2.0	2/1/2022	Dennis Lauer	Approval
2.1	2/22/2023	David Oluyitan	Annual review and update of password policy – at least 10 characters; never expire; 5 reuse generation
3.0	2/28/2023	Dennis Lauer	Approval