




Information Technology Access Control Policy

February 28, 2023



Prepared by:
David Oluyitan,
Senior Manager,
Information Assurance

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

Access Control Policy

1. Purpose

The purpose of the IT Access Control policy is to provide direction to adequately protect all “Cadmus” information systems from unauthorized or inappropriate access. Cadmus includes employees, contractors, and consultants who maintain network credentials and have access to the information systems and networks of The Cadmus Group, Obsidian Analysis, LLC, Cadmus International LLC., Meister Consulting Group. Access to Cadmus information systems is limited to authorized persons whose job responsibilities require their use. Access is given through the establishment of a unique account in accordance with Cadmus Access Control Procedures. To comply with U.S Federal regulations, Cadmus establishes, implements, and enforces access control policies and procedures consistent with the access controls in the National Institute of Standards for Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy controls for Federal Information Systems and Organizations. This control set provides the basis for this policy and applies to all Cadmus.

Firm users are required to be familiar with, and abide by, policies, standards, and rules of behavior. The policies, rules of behavior, and standards provide appropriate and acceptable usage of Cadmus Critical Systems. All Cadmus users will have access to and be required to complete annual security awareness training; and materials related to information security. All Cadmus users must maintain the confidentiality of information assets even if technical security mechanisms fail or are absent. Cadmus users (e.g., employees, consultants, and contractors) are obligated to report instances of non-compliance.

2. Scope

This policy applies to:

- a) 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 (Cadmus).
- b) Client or government data, in any medium or form, generated, collected, provided, transmitted, stored, maintained, or accessed by, or on behalf of, Cadmus.
- c) Information systems or services (including cloud-based services) owned, used, or operated by Cadmus.
- d) Interconnections between or among Cadmus information systems.

3. Dissemination

This policy is available only to designated individuals within Cadmus with a need-to-know on the internal SharePoint site (e.g., Firm employees and contractors). The policy is specifically disseminated to members of the following teams: IT Client Services (CS), Engineering & Operations

(ENO), Architecture & Systems Design (ASD), Information Assurance, Chief Information Officer (CIO), and also Cadmus Executive Leadership.

4. Account Management [NIST SP 800-53, AC-2]

Cadmus system owners establish, maintain, and document a user account procedure to administer user accounts for all applicable information systems developed, maintained, or operated by Cadmus employees, contractors, and others working for, or on behalf of, Cadmus.

The account management procedure:

- a) Identifies account types (e.g., individual, group, system, application, contractor, and vendor)
- b) Assigns account manager (for Contractors only)
- c) Establishes conditions for group membership (i.e., SharePoint and Security Groups)
- d) Identifies authorized users of information systems and specify access privileges
- e) Specifies necessary approvals for requests to establish accounts
- f) Outlines a process for establishing, activating, modifying, disabling, and removing accounts
- g) Specifically document the process for the issuance/revoking of contractor accounts
- h) Details process for contractor account revocations. IT schedules contractor account revocations per notification from Cadmus Contracts Department and/or Contract Manager/POC when accounts are no longer required or prior to the contract end date (specified in contractor form)
- i) Establishes conditions for notifying account managers:
 - When accounts are no longer required
 - When users are terminated or transferred
- j) Deactivates accounts that are no longer valid
- k) Authorizes access to information systems based on:
 - A valid access authorization
 - Intended system usage
 - Other attributes as required to perform business functions
- l) Establishes an annual review of accounts for compliance with requirements. Normal accounts are reviewed quarterly (i.e., Offboarding Requests) and elevated accounts are reviewed annually (i.e., Privileged Accounts)

(1) Automated Account Management [NIST SP 800-53 AC-2(1)]

- a. Cadmus employs automated mechanisms to support the management of information system accounts. Monitoring tool alerts for AD account password expirations and automation for account creations (AD Manager).

(2) Removal of Temporary and Emergency Accounts [NIST SP 800-53, AC-2(2)]

- a. Cadmus System Owners manually disable or remove temporary (contractor) and emergency accounts, if applicable, after a ninety (90) day period and accounts are offboarded and removed after a period of 180 days.

(3) Disable Inactive Accounts [NIST SP 800-53, AC-2(3)]

- a. Cadmus manually disables user accounts after ninety (90) days of inactivity.

(4) Automated Audit Actions [NIST SP 800-53, AC-2(4)]

- a. Cadmus information systems are configured to automatically audit all account creation, modification, enabling, disabling, and removal actions. Cadmus information system owners will only be notified for privileged account creation or deletion.

(5) Inactivity Lockout

- a. Cadmus information systems are configured to lock out after an organization-defined time period of expected inactivity. Time period can differ for various applications except Cadmus laptops, which initiates lock out after thirty (30) minutes of inactive use.

See the Access Control Procedures for detailed information.

5. Access Enforcement [NIST SP 800-53, AC-3]

- a) Cadmus employs mandatory access enforcement mechanism(s) to implement access control policies to ensure that:
 - (1) Only authorized individuals may access objects in accordance with information system access control policies. For example, only authorized individuals and software components may access specific information and information resources.
- b) Cadmus develops System Security Plans (SSPs) for Critical Systems to identify and document system functions, privileged commands, accesses, and other specified actions that require dual authorization.
- c) Cadmus enforces a dual account creation approval process (i.e., Contract Manager and CIO) for contractor user access to Cadmus information systems.

6. Information Flow Enforcement [NIST SP 800-53, AC-4]

Cadmus implements information flow control measures to enforce where and how information is allowed to travel within an information system and between interconnected information systems. This includes:

- a) Enforcing remote access restrictions.
- b) Enforcing the use of default firewall rules as a basis for flow of control decisions.
- c) Preventing unauthorized communication between designated sources and destinations (e.g., individuals, devices, networks).
- d) Enforcing IP address matching for routing purposes.
- e) Enforcing anti-spoofing measures to detect and block source IP addresses from entering the network.
- f) Enforcing stateful inspection (dynamic packet filtering).

7. Separation of Duties [NIST SP 800-53, AC-5]

Cadmus:

- a) Separates duties based on responsibilities and departments so that the potential for abuse of authorized privileges and risk of malevolent activity without collusion is minimized.
- b) Implement separation of duties for all systems through assigned information system access authorizations to ensure a sufficient level of separation of duties is implemented so that a single

individual cannot perform combinations of functions that could result in a conflict of interest, fraud, or abuse.

8. Least Privilege [NIST SP 800-53 AC-6]

Cadmus employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Cadmus implements the principles of least privilege, ensuring that:

- a) Privileged users permitted to access security functions in hardware, software, or firmware, and security relevant information will use non-privileged accounts or roles when accessing non-security features.
- b) Privileged accounts and groups are only used to perform privileged job functions.

(1) Authorize Access to Security Functions

- a. Cadmus explicitly authorizes all security functions and security-relevant information to Cadmus IT Team (IT Ops Manager, Engineering Ops Lead, Senior Cloud Architect, System Administrators, IT Client Services, etc.) and other privileged users. Security functions include, but are not limited to:
 - Account creation
 - Access authorizations
 - Setting events to be audited
 - Setting intrusion detection parameters
 - Network configuration (deployed in hardware, software, firmware)

(2) Non-Privileged Access for Non-Security Functions

- a. Cadmus ensures that privileged accounts are used only when necessary to perform system administration and security functions. Users use non-privilege accounts when conducting non-system administration or security actions.

(3) Privileged Accounts

- a. Cadmus restricts privileged accounts on information systems to IT Ops Manager, Engineering Ops Lead, Senior Cloud Architect, System Administrators, IT Client Services, or other personnel or roles with an approved justification.

(4) Review of User Privileges

- a. Privileged user accounts are reviewed annually, in which privileges are reassigned or removed as necessary to reflect business needs.

(5) Auditing Use of Privileged Functions

- a. Cadmus is required to establish a process for linking all access to systems, including administrative privileged accounts (e.g., root or administrator) to each individual user. **Note: All service account credentials are stored in a password management software that only authorized information system owners have access to.**

- b. Cadmus information systems create audit records when a privileged command is performed, or a privileged account makes a security-related change to Cadmus information systems, such as creating an account or group, assigning roles and privileges to an account or group, or changing account or group privileges.

(6) Prohibit Non-Privileged Users from Executing Privileged Functions

- a. Configuration settings in Cadmus information systems prevent non-privileged users and accounts from executing privileged functions, including disabling, circumventing, or altering security safeguards and countermeasures, such as performing system integrity checks or cryptographic key management activities.

9. Unsuccessful Login Attempts [NIST SP 800-53, AC-7]

Cadmus information systems are configured to:

- a) Enforce a limit of ten (10) consecutive invalid login attempts by a user during a thirty (30) minute time period.
- b) Automatically lock privileged and non-privileged accounts and delay the next login prompt for thirty (30) minutes when the maximum number of unsuccessful login attempts is exceeded. Users are permitted to reach out to IT Client Services (Help Desk) to release their account prior to the thirty (30) minute lock out period if the lock out hinders productivity.

10. System Use Notification (Logon Banner) [NIST SP 800-53, AC-8]

Cadmus information systems:

- a) Display a Firm-approved notification banner at logon before granting individuals access to information systems owned by, or operated on behalf of, Cadmus. The banner will display references, if any, regarding monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
- b) Include a description of the authorized uses of the system.

11. Session Lock [NIST SP 800-53, AC-11]

Cadmus configures information systems to initiate a session lock to prevent further access to the system:

- a) After thirty (30) minutes of inactivity.
- b) Until the user reestablishes access using established identification and authentication procedures.
- c) Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

12. Session Termination [NIST SP 800-53, AC-12]

Cadmus information systems are configured to lock out users during a session:

- a) After a period of inactivity defined by System owners for each applicable system. **Note: System owners have varying requirements based on system use. Refer to the applicable System Security Plan for the listing of requirements for each Critical System.**

- b) System owners coordinate session termination configurations in consultation with Cadmus IT Management and the system host(s). Exemptions for specific user accounts or devices will require a waiver request approved by Cadmus Change Control Board (CCB).

13. Remote Access [NIST SP 800-53, AC-17]

Remote access encompasses any connection to Cadmus information systems or components originating from outside of Cadmus owned and operated network infrastructure, such as accesses for telework and mobile work.

Cadmus:

- a) Identifies the approved remote access methods for users to access Cadmus information systems.
- b) Establish usage restrictions, configuration and connection requirements, and implementation guidance for the permitted remote access methods and document them in the SSP.
- c) Immediately deactivate subcontractor and service provider remote access no later than contract end date. Contracts Point of Contact (POC) notifies Cadmus IT if there is an earlier end date.

(1) Protection of Confidentiality/Integrity Using Encryption

- a. Ensure that remote access methods:
 - (1) Employ NIST FIPS PUB 140-2, *Security Requirements for Cryptographic Modules* certified encryption.
 - (2) Transmit and transfer data via an encrypted channel in compliance with Cadmus Information Technology Standards documentation (Section: Encryption Standards).

(2) Managed Access Control Points

- a. Cadmus routes all remote access sessions through Cadmus-authorized access control points.

(3) Privileged Commands and Access

- a. Cadmus documents and set conditions (e.g., HTTPS, VPN, encrypted channels) for the execution of privileged commands and access to security-relevant information via remote access methods.

14. Wireless Access [NIST SP 800-53, AC-18]

Cadmus:

- a) Establish usage restrictions, configuration and connection requirements, and implementation guidance for wireless access and document them in the SSP.
- b) Manually monitor corporate wi-fi unauthorized access.
- c) Authorize wireless access to the information system or network via wireless keys prior to allowing such connections.

(1) Authentication & Encryption

- a. Cadmus protects wireless access to information systems using WPA2/PSK authentication.

15. Access Control for Mobile Devices [NIST SP 800-53, AC-19]

The requirements in this section apply to Cadmus-owned or controlled devices. *Section 15* provides access requirements for client devices that are not Cadmus-owned or controlled.

Cadmus:

- a) Establishes usage restrictions; device identification, integrity, and configuration requirements in accordance with the Bring Your Own Device (BYOD) Policy; authentication and connection requirements; and implementation guidance for each type of laptop and mobile device consistent with the BYOD Policy; usage restrictions and implementation guidance for company-owned mobile devices.
- b) Authorize the connection of mobile devices to organizational information systems using multifactor authentication (MFA).
- c) Monitor unauthorized connections of mobile devices to organizational information systems for suspicious IP addresses and locations.

16. Use of External Information Systems [NIST SP 800-53, AC-20]

- a) Requirements in this section do not apply to external information systems that access public interfaces to Cadmus information systems, including publicly accessible Firm websites.

(1) Limits of Authorized Use

- a. Cadmus permits the use of external information systems to process, store and/or transmit company information only when:
 - A valid business reason exists for the external trust relationship.
 - A formal risk assessment of the third-party has been conducted.
 - Risks identified in the risk assessment have been adequately addressed, if applicable.
 - A formal contract exists, including Non-Disclosure Agreements (NDAs).

(2) Portable Storage Device (PSD)

Cadmus:

- a. Limits the use of Firm-controlled portable storage devices except by authorized individuals on external information systems.
- b. Prohibits the use of portable storage devices in Cadmus information systems when such devices have no identifiable owner.
- c. Prohibits personally owned portable storage devices on external information systems.

Refer to Cadmus Rules of Behavior for more information.

17. Information Sharing [NIST SP 800-53, AC-21]

Cadmus:

- a) Ensures personnel involved in the information sharing process are trained on their roles (i.e., handling, or sharing sensitive information or Controlled Unclassified Information), as needed.
- b) Establishes procedures that may require qualified personnel to review or approve information prior to being released or may require a signed memorandum of agreement with an external party prior to sharing the information.
- c) Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner are consistent with the access restrictions on the client and company confidential or PII information.
- d) Employs Data Loss Prevention (DLP) to assist Cadmus in monitoring information sharing and collaboration.

18. Publicly Accessible Content [NIST SP 800-53, AC-22]

Cadmus:

- a) Designates individuals authorized to post information on publicly accessible Firm information systems.
- b) Trains individuals to ensure that publicly accessible information does not contain non-public information.
- c) Ensures only authorized users post information approved for public release.
- d) Performs a series of reviews and approval of proposed content/information prior to posting onto the publicly accessible information system to ensure that only public information is included.
- e) Conducts regular reviews of the content on the publicly accessible information system for nonpublic information and remove this information, if discovered.

APPENDIX A: GLOSSARY

Access Control – An entire set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access based on pre-established rules.

Access Control Policies – Specify how to control accesses between subjects (e.g., individuals or software acting on behalf of individuals) and objects (e.g., information, information systems, and components of information systems) in information systems.

Authentication – Verifying the identity of a user, process, or device as a prerequisite to allowing access to resources in an information system. (Source: NIST, SP 800-53, Revision 4)

Authorization. Access privileges granted to a user, program, or process or the act of granting those privileges.

Automated Mechanism – A software function with characteristics that results in increasing the efficiency, chance of a desired outcome, or reducing the risk of failure or manipulation, in an entire, or a part of, a process.

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.

Controlled Unclassified Information (CUI) – Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. (Source: EO 13556, Controlled Unclassified Information)

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.

Dual Authorization (Dual Control) – A process that uses two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. No single entity is able to access or use the materials, e.g., cryptographic keys. (Source: NIST, SP 800-57)

Encryption – A security mechanism that renders information unintelligible to unauthorized persons and allows the information to be restored to its plain-text format by authorized persons.

Firewall – A device that has a network protection application installed to safeguard the network from intentional or unintentional intrusion. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet. (Source: NIST, SP 800-35)

Group – An object in an authentication system where a collection of accounts is associated that shares common access attributes or privileges based on job function. For example, personnel that maintain an application have their accounts associated with an administrator group and are granted the attributes and privileges assigned to the group.

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)

Mandatory Access Control – Access control policy decisions are made by a central authority, not by the individual owner of an object. Users cannot change access rights. An example of mandatory access control occurs in military security, where an individual data owner does not decide who has a top-secret clearance, nor can the owner change the classification of an object from top-secret to secret. (Source: NIST, SP 800-192)

Mobile Device – A small mobile computer such as a smartphone or tablet. (Source: NIST, SP 800-46, Revision 2)

Mobile Work – Work which is characterized by routine and regular travel to conduct work in customer or other worksites as opposed to a single authorized alternative worksite. Examples include site audits, site inspections, investigations, property management, and work performed while commuting, traveling between worksites, or on temporary duty. Mobile work is not considered telework; however, mobile workers may be eligible to participate in telework, as applicable.

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)

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

Privileged Command – A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. (Source: NIST, SP 800-53, Revision 4)

Privileged User – A user that is authorized (and therefore, trusted) to perform security relevant functions that ordinary users are not authorized to perform. (Source: NIST, SP 800-53, Revision 4)

Remote Access – The ability for an organization's users to access its non-public computing resources from external locations other than the organization's facilities. (Source: NIST, SP 800-46, Revision 2)

Remote Access Method – Mechanisms that enable users to perform remote access. There are four types of remote access methods: tunneling, portals, remote desktop access, and direct application access. (Source: Adapted from NIST, SP 800-46, Revision 2)

Separation of Duties – A security principle that divides critical functions among different staff members to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud. (Source: NIST, SP 800-57)

Session Lock – A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system level but may be at the application level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workdays. (Source: NIST, SP 800-53, Revision 4, see control AC-11 - supplemental guidance)

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)

Telework – The term “telework” or “teleworking” refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee’s position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work.

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.

Virtual Private Network (VPN) – A virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks. (Source: NIST, SP 800-46, Revision 2)

RECORD OF CHANGES

This section documents the changes made to Cadmus Information Technology (IT) Access Control policy.

Version	Date	Author	Description of Changes
0.1	12/19/2019	Matt Pierce	Initial draft
0.2	10/23/2020	David Oluyitan, John O’Keeffe , Ahmed Rafeq, Erik Stillman,	IT Policy Updates for 2020 Workshop Session
0.3	10/28/2020	Oluyitan, O’Keeffe, Rafeq, Stillman	IT Policy Updates for 2020 Workshop Session II
0.4	10/30/2020	Oluyitan, O’Keeffe, Rafeq, Stillman, Dustin Hermann	IT Policy Updates for 2020 Workshop Session III
0.5	11/02/2020	Dennis Lauer, CIO	Exec. mgmt. comments for the Policy reform team; comprehensive review, and updates to each section
0.6	11/05/2020	Oluyitan, O’Keeffe, Rafeq, Stillman, Hermann	IT Policy Updates for 2020 Workshop Session IV
1.0	12/8/2020	Dennis Lauer	Final review and approval
1.1	1/20/2022	David Oluyitan, Erik Stillman	Annual review and updates
2.0	1/20/2022	Dennis Lauer	Approval
2.1	2/28/2023	David Oluyitan	Annual review and updates
3.0	2/28/2023	Dennis Lauer	Approval