Title: Access Control Standard
Owner: Owner of Standard/Policy
Document #: Assigned Control #
Version: 1.0 **Date:** MM/DD/YYYY **Pages:** **1 of 9**

CHICAGO METRICS
Process | People | Technology

Purpose

This document establishes the Access Control Standard for managing security controls, ensuring proper access and denying unauthorized access to **ORGANIZATION NAME** information systems. This standard reflects applicable local, state and federal laws and regulations, and **ORGANIZATION NAME** policies.

Authority Statement

This standard is issued by the **ORGANIZATION NAME TITLE** in accordance with the authority granted under the **NAMED** Policy, **CONTROL NUMBER**.

Framework/Regulatory Alignment

NIST 800-53: AC-2(1)(2)(3)(4)(5)(12)(13), AC-3, AC-4, AC-5, AC-6(1)(2)(5)(6)(7)(9)(10), AC-7, AC-8, AC-11(1), AC-12, AC-14, AC-17(1)(2)(3)(4)(9), AC-18(1)(4)(5), AC-20(1)(2), AC-21, AC-22
FERPA: 34 CFR § 99.31 (a)(1)(ii)
HIPAA: 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(a)(2)(iv)
AOPO: IT 2.2, IT 2.5, IT 2.7
PCI: 1.1, 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6, 1.1.7, 1.2, 1.2.1, 1.2.2, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.4, 2.1.1, 2.2.5, 2.3, 2.6, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.3, 4.1, 4.1.1, 6.4, 6.4.2, 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3, 8.1, 8.1.1, 8.1.2, 8.1.2, 8.1.3, 8.1.3, 8.1.4, 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.1.8, 8.2, 8.2.2, 8.3, 8.5, 8.5.1, 8.6, 8.7, 8.8, 9.1, 9.1.3, 9.5, 9.6, 9.6.1, 9.6.3, 9.7, 9.9, 9.9.2, 10.1, 10.2, 10.2.1, 10.2.2, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.3.7, 10.5, 10.6, 10.6.1, 10.6.2, 10.6.3, 10.7, 11.1, 11.4, 11.5, 12.3, 12.3.1, 12.3.2, 12.3.5, 12.3.8, 12.3.9, 12.3.10, 12.8.3, A.1.1, A.1.3

Scope

This standard applies to all users who access **ORGANIZATION NAME** information systems. Information system account types include, but are not limited to: individual, shared, group, temporary, and guest.

Standard

1) **Account Management**

NIST 800-53: Low: AC-2, Mod: AC-2(1)(2)(3)(4), High: AC-2(1)(2)(3)(4)(5)(12)(13)
HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii)
AOPO: IT 2.7
PCI: 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3, 8.1.5, 8.1.6, 8.1.7, 8.1.8, 8.3, 8.7, 8.8, 9.1, 9.6.1, 12.3.8, 12.3.9, 12.3.10, A.1.1

a) AC-2(a): The following types of information system accounts shall be identified and selected to support business functions:
  i) ERP
  ii) Financial Systems
  iii) Human Capital Systems
  iv) Activation, Authorization, Authentication Systems (Active Directory)
  v) **OTHER BUSINESS SYSTEMS**

b) AC-2(b): Account managers shall be assigned for information system accounts.

c) AC-2(c): Conditions for group and role membership shall be established.

d) AC-2(d): Authorized users of information systems, group and role membership, and access authorizations (e.g., privileges) and other attributes shall be specified for each account as required.

e) AC-2(e): Requests to create information system accounts shall require approval:
  i) Standard user accounts require HR approval and set up account names to be created automatically.
  ii) Administrative accounts depend on the system requiring access but should include the approval of the Director over that system and may require approval of the Information Security Office depending on the level of access as prescribed in the **Privileged Account Access Standard**.

f) AC-2(f): Information system accounts shall be created, enabled, modified, disabled and removed in accordance with **ORGANIZATION NAME** standards, procedures and guidelines.

g) AC-2(g): Use of Information system accounts shall be monitored, logged and reviewed periodically.

h) AC-2(h): Account managers shall be notified, by the manager of a terminated or transferring employee, when accounts are no longer required, when users are terminated or transferred and when individual information system usage or need-to-know changes.

i) AC-2(i): Access to information systems shall be authorized based on valid access authorization, intended system usage and other attributes as required by associated job functions.

j) AC-2(j): Accounts shall be reviewed for compliance with account management requirements at least **TIME PERIOD**.

k) AC-2(k): A process for re-issuing shared/group account credentials shall be established when individuals are removed from the group.

l) AC-2(1): Automated mechanisms shall be used to support the management of information system accounts including provisioning and deprovisioning and transfers.

m) AC-2(2): Information systems automatically disables temporary and emergency accounts after **TIME PERIORD** unless extended by user's supervisor with proper authority.

n) AC-2(3): Information systems automatically disables inactive accounts after, no longer than **TIME PERIOD**.

o) AC-2(4): Information systems automatically audit account creation, modification, enabling, disabling and removal actions and notify **DEFINED PERSON(S)**.

p) AC-2(5): Users shall log out or lock the device when not actively working in systems. Systems shall log users out after no more than **TIME PERIOD** of inactivity.

q) AC-2(12): Information systems shall be monitored and unusual activity reported to the Information Security Office.

r) AC-2(13): Accounts of users posing a significant risk shall be disabled within four (4) hours of discovery of risk.

2) Access Enforcement

NIST 800-53: Low: AC-3, Mod: AC-3, High: AC-3
HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)
AOPO: IT 2.7
PCI: 1.1, 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6, 1.1.7, 1.2, 1.2.1, 1.2.2, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 2.1.1, 2.3, 2.6, 4.1, 4.1.1, 8.1.5, 8.3, 9.1.3, 11.1, 11.4, 12.3.9, 12.8.3

a) Information systems shall enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

3) Information Flow Enforcement

NIST 800-53: Low: N/A, Mod: AC-4, High: AC-4
HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.310(b)
AOPO: IT 2.7
PCI: 1.2.1, 8.1.5, 8.3, 12.3.9

a) Information systems shall enforce approved authorizations for controlling the flow of information within the systems and between interconnected systems based on **ORGANIZATION NAME** standards, procedures and guidelines.

4) Separation of Duties

NIST 800-53: Low: N/A, Mod: AC-5, High: AC-5
HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.312(a)(1)
AOPO: IT 2.7
PCI: 1.1, 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6, 1.1.7, 1.2, 1.2.2, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 2.1.1, 4.1.1, 9.1.3, 9.9, 9.9.2, 11.1, 11.4

a) Terms and conditions shall be established and consistent with any trust relationships established with other organizations owning, operating and/or maintaining external information systems, allowing authorized individuals to:
  i) access information systems from external information systems; and
  ii) process, store or transmit **ORGANIZATION NAME**-controlled information using external information systems.

b) AC-20(1): Authorized individuals shall be permitted to use external information systems to process, store or transmit **ORGANIZATION NAME**-controlled information only when:
  i) the implementation of required security controls on the external system is verified or risk accepted; **and**
  ii) approved information systems connections or processing agreements with the organization hosting the external information system is retained.

c) AC-20(2): The use of **ORGANIZATION NAME**-controlled portable storage devices by authorized individuals on external information systems is restricted.

16) Information Sharing

NIST 800-53: Low: N/A, Mod: AC-21, High: AC-21
HIPAA: N/A
AOPO: IT 2.7
PCI: 9.6.1, 12.3.1

a) AC-21(a): Authorized users shall determine whether access authorizations assigned to entities with which information is to be shared match the access restrictions on the information.

b) AC-21(b): Processes shall be employed to assist users in making information sharing decisions. **<INSERT DATA CLASSIFICATION STANDARD>**

17) Publicly Accessible Content

NIST 800-53: Low: AC-22, Mod: AC-22, High: AC-22
HIPAA: N/A
AOPO: IT 2.7
PCI: 8.1.6, 8.1.7

a) AC-22(a): Individuals authorized to post information onto publicly accessible systems shall be designated to do so.

b) AC-22(b): Individuals authorized to post information onto publicly accessible systems shall be trained to ensure non-public information (e.g., PII/PHI) is unavailable to unauthorized users.

c) AC-22(c): The proposed content of information shall be reviewed prior to posting onto publicly accessible systems to ensure that non-public information (e.g., PII/PHI) is not included.

d) AC-22(d): The content on publicly accessible systems shall be reviewed **TIMEFRAME** for non-public information and removed if discovered.

Exceptions

Exceptions to this standard may be authorized, when:

1) Documented (e.g., Service Desk ticket);
2) Recommended by the **RISK TEAM or OTHER GROUP**; **AND**
3) Approved by the **CIO**/**CRO**/**CISO**.

Non-Compliance

In accordance with **ORGANIZATION NAME** Rules and Policies, users failing to comply with this standard shall be subject to discipline, up to and including dismissal.

Revision History

Version	Change	Author	Date of Change
1.0	Initial Version	**NAME**	**DATE**