

# 9400-P173: Logical Access Controls on IT Resources

## I. PURPOSE

This policy prescribes the circumstances for the request and requirements for the enforcement of identification and authentication (I&A) controls such as user IDs and passwords.

## II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as “agencies”) and to all user-accessible systems (hardware and software that process data in a meaningful way) managed by these agencies, which includes applications, peripherals, removable media, other components and could be one computer or a network of computers.

## III. POLICY

- A. Logical access controls shall be employed whenever there is a requirement to differentiate between levels of access privileges and/or authorized and unauthorized users to agency information or information technology resources.
- B. Whenever logical access controls are needed, at least one technical component must ask for the requestor’s identification (UserID) and successfully validate the authentication (password) before the requested information or service can be accessed.
- C. The use of stronger, two-factor authentication mechanisms (such as those that employ single-use password tokens or biometrics) for critical or sensitive systems shall be considered (see Policy 8100-P131: Information Classification).
- D. Common policies for all implementations of logical access controls shall be:
  - 1. Systems that request UserIDs and passwords shall mask, suppress, or otherwise obscure the display and printing of passwords so that unauthorized parties will not be able to observe or subsequently recover them.
  - 2. If any part of the login sequence is incorrect, the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the login process was incorrect.
  - 3. The number of unsuccessful logon attempts shall be limited. Users that are unsuccessful at logging on within the prescribed number of tries shall be locked out for a prescribed period of time.
  - 4. Access controls that cannot distinguish between authorized and unauthorized users must default to denial of access and privileges.
  - 5. Access to system utilities shall be limited to users and administrators with an approved need to run or use those utilities. Other uses of and access to

## 9400-P173: Logical Access Controls on IT Resources

those utilities shall be granted on a temporary basis only after a business requirement for this access has been documented and approved. Unneeded system utilities, options, and/or services shall be removed or disabled.

6. Log on warning banners shall be displayed during initiation of the login process to networks and where appropriate, to other resources prior to requests for UserIDs and passwords. Warning banner formats are specified in Standard 9400-S173: Security Warning Banner.
  7. Screen savers (sometimes called “screen locks”) shall be automatically activated and password protected on terminals after a prescribed period of inactivity.
- E. Access controls for operating systems and database management systems.
1. System and database administrators shall configure operating systems and databases to implement and enforce applicable password management requirements.
  2. All users and other entities (applications, systems, etc.) must be uniquely identified to the information system(s) they access and shall only have access to resources for which they have been explicitly authorized.
  3. Direct connections from the Internet to internal, non-public, database systems, even to view data, shall not be allowed. This does not include third parties supporting database management or other maintenance, provided they are connecting via a protected path.
- F. Application access controls. The following controls shall be employed on applications under an agency’s development control to restrict access to information.
1. Third party applications (to the greatest extent possible) and custom written applications shall utilize technical security controls available through operating systems or database management systems. When this is not possible, applications shall provide the access controls.
  2. UserIDs and passwords that are “hard coded” in applications shall not be linked to individuals or permitted without review and approval by the data steward or designee.
  3. To the extent possible, critical or sensitive applications shall be hosted on servers (including virtual systems) that are dedicated to the purpose of hosting sensitive and/or critical applications.
- G. Access to information and information systems shall be internally audited in a manner commensurate with the value of the resources being protected and should:

## **9400-P173: Logical Access Controls on IT Resources**

1. Assure all security administration activity is recorded and reported for review.
2. Detect and report security violations.
3. Provide ways to recover current and historical information about security administration in the event of a system failure.
4. Identify all users and their access capabilities without disclosing their passwords (i.e., general users, advanced users, and administrator).
5. Be able to establish a user's accountability for their actions on the protected information system.

**CIO Approved Date: 06/17/2009**