Ohio Supercomputer Center Password PIN Security	**No:** **OSC-8**
	Effective: **06/01/2009**
	Issued By: Kevin Wohlever Director of Supercomputer Operations **Published By:** Ohio Supercomputer Center **Original Publication Date:** TBD

1.0 Purpose

This policy establishes minimum requirements regarding the proper selection, use and management of passwords and personal identification numbers (PINs). References in this policy to passwords also apply to PINs, except where explicitly noted.

2.0 Scope

Pursuant to Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," this policy applies to all systems under the control of the Ohio Supercomputer Center.

The scope of this information technology policy includes OSC computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the state who use and administer such systems.

3.0 Background

The first line of defense in computer system security is the user – anyone having authorized access to computer systems and networks. Breach of user passwords is one of the easiest methods of gaining unauthorized access to sensitive information and systems. Proper password management is one of the most effective, most cost effective and most necessary measures in restricting unauthorized access.

4.0 References

4.1 Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," defines the authority of the state CIO to establish State of Ohio IT policies as they relate to state agencies' acquisition and use of information technology, including, but not limited to, hardware, software, technology services and security.

4.2 Chapter 1306 of the Ohio Revised Code and Rule 123:3-1-01 of the Ohio Administrative Code specifically govern the use of legally binding records and signatures in electronic formats and includes companion security requirements to this policy.

4.3 OSC IT Policy, OSC-3, "Information Security Framework," is the overarching umbrella security policy for OSC information and services. OSC IT Policy OSC-83, "Password and PIN Security," is one of several subpolicies. These security policies should be considered collectively rather than as separate or unrelated.

4.4 Ohio IT Policy ITP-B.7, "Security Incident Response," requires the state and its respective agencies to develop and maintain an adequate security response capability for identified security incidents.

4.5 A glossary of terms found in this policy is located in Section 9.0 - Definitions. The first occurrence of a defined term is in ***bold italics***.

5.0 Policy

5.1 Composition. Ensure that password composition is commensurate with the ***risk assessment*** of the ***system assets*** being protected. Data requiring secure access shall have passwords composed of upper and lower case letters, numbers and special characters.

5.2 Length. Ensure that the length of passwords is commensurate with the risk assessment of the system assets being protected. Longer passwords shall be utilized for information or assets requiring more security.

5.3 Aging. Passwords shall have a lifetime commensurate with the risk assessment of the system assets being protected. Passwords for higher risk assets shall have a shorter lifetime.

5.4 System Lockout. OSC shall establish a maximum number of allowed password attempts commensurate with the risk assessment of the system assets. Upon exceeding the prescribed number of unsuccessful attempts, the user account or terminal activity shall be suspended.

5.5 System Lockout Reset. Commensurate with the risk assessment of the system assets, a policy on the method of reinstating a user account subject to system lockout. For systems having higher risk assets, users with a suspended account shall be re-authenticated before access is reactivated. For systems having lower risk assets, a reset feature may be used before the account is automatically reactivated, such as having a predetermined time lapse or prompting the user to provide a piece of additional information that only he or she would know.

5.6 History. Passwords shall have a re-use period commensurate with the risk assessment of the system assets being protected.

5.7 ***Source***. OSC shall designate persons responsible for creating or selecting passwords for each system.

5.8 Uniqueness. When secured access is used, the combination of user-ID and personal password shall authenticate a unique user. User accounts for OSC controlled systems will be associated with a single individual and shall not be established for use by more than one person.

5.9 Storage. Agencies shall maintain and safeguard system password files in a manner to prevent unauthorized access. Password files will be backed-up to facilitate recovery from system failures, security breaches, disasters, accidents and like events with the potential to affect systems.

5.10 Transmission. Electronic transmission of passwords from one destination to another shall be protected from unauthorized access at a level commensurate with the risk assessment of the system asset.

5.11 Deactivated Passwords. Passwords of employees, contractors, temporary personnel and other agents of OSC, who have terminated or transferred to other work units shall be deactivated. Passwords will be deactivated for such users no later than the end of business on the effective date. A terminated user's passwords shall not be retained beyond termination date. Passwords associated with involuntary terminations shall be deactivated immediately upon notification.

5.12 Compromised Passwords. Passwords compromised maliciously or by accident shall be deactivated immediately. All instances of maliciously compromised passwords should be immediately reported in accordance with the OSC security incident reporting policy as defined in OSC IT Policy OSC-7, "Security Incident Response."

5.13 Save Password Option. OSC shall avoid system and application configurations that allow for the use of ***save password options***. If a system's "save password" feature cannot be disabled, users shall be instructed not to use that option.

5.14 Administrative Accounts

5.14.1 Operating systems not requiring user-IDs, passwords or other security measures for access to administrative level services shall be identified and procedures developed to offset this vulnerability. OSC shall ensure that administrators of such systems are both aware of the vulnerability and trained in how to safeguard such systems. Upgrades to these systems shall include security measures to include user-IDs and passwords.

5.14.2 If supported by the operating system, administrator groups shall be established and only authorized personnel shall be assigned to these groups. All other users shall be restricted from accessing administrator accounts.

5.14.3 Only Authorized personnel should be issued administrative accounts. Those with authorized administrative accounts shall use separate user accounts for non-system administrator tasks.

5.15 Display. Passwords shall be hidden from display at all times.

5.16 Distribution and Training. OSC shall ensure that the distribution of passwords maintains confidentiality, integrity and availability. Passwords shall only be permitted for authorized users pursuant to OSC IT Policy OSC-3, "Information Security Framework Policy."

Users shall be instructed that: the protection of passwords is the responsibility of each user; users will safeguard and keep their passwords confidential; personal information such as social security number, meaningful dates, nicknames or other obvious information shall not constitute a password.

5.17 Password Testing. OSC will randomly and regularly test password effectiveness. Password testing will be conducted by authorized personnel only and should occur at least annually.

5.18 Default Passwords. Default application and system passwords shall be reset before deployment of any system or application.

6.0 Procedures

None.

7.0 Implementation

This policy is effective immediately.

8.0 Revision History

Date	Description of Change
6/1/2009	Original policy.

9.0 Definitions

9.1 Password Aging. The period of time after which a password is no longer considered secure. Typically, the older the password, the less secure it is.

9.2 Password Composition. The types of characters such as upper and lower case letters, numbers and special characters that comprise a password.

9.3 Password Length. The number of characters in a password. The longer the password, the more secure it is.

9.4 Risk Assessment. A process concerned with identifying, analyzing and responding to IT security risks. Risk assessment attempts to maximize the results of positive events and minimize the results of negative events. See Ohio IT Policy ITP-B.1, “Information Security Framework,” for assessment guidelines.

9.5 Save Password Option. An option on some systems that, when enabled, allows the user the choice of whether to have the user password memorized by the system so that it will not need to be re-entered upon subsequent access.

9.6 Source. An entity that can create or select a valid password.

9.7 System Assets. System assets include information, hardware, software and services required to support the business of the agency, and identified during the risk assessment process as assets that need to be protected in accordance with Ohio IT Policy ITP-B.1, “Information Security Framework.”

10.0 Related Resources

None

11.0 Inquiries

Direct inquiries about this policy to:

Director of Supercomputer Operations
1224 Kinnear Rd.
Columbus, OH 43212

Telephone: 614-292-9248

OSC IT Policies can be found on the Internet at: www.osc.edu/policies