



<h2 style="margin: 0;">State of Ohio IT Policy</h2> <p style="margin: 0;">Password and Personal Identification Number Security</p>	No: <h3 style="margin: 0;">ITP-B.3</h3>
	Effective: <h3 style="margin: 0;">03/19/2008</h3>
	Issued By: R. Steve Edmonson Director, Office of Information Technology State Chief Information Officer Published By: Statewide IT Policy Investment and Governance Division Original Publication Date: 12/05/2002

1.0 Purpose

This policy establishes minimum requirements for state agencies 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 state policy applies to every organized body, office, or agency established by the laws of the state for the exercise of any function of state government except for those specifically exempted.

The scope of this information technology policy includes state 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, defined for the purposes of this policy as anyone with 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 to restrict 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 chief information officer 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 include companion security requirements to this policy.
- 4.3 Ohio IT Policy ITP-B.1, "Information Security Framework," is the overarching umbrella security policy for state information and services. Ohio IT Policy ITP-B.3, "Password and Personal Identification Number Security," is one of several subpolicies. These security policies should be considered collectively rather than as separate or unrelated policies. Attachment 1 illustrates the interrelationship of state technology security policies.
- 4.4 Ohio IT Policy ITP-B.7, "Security Incident Response," requires the state and its agencies to develop and maintain an adequate security response capability for identified security incidents.
- 4.5 Ohio IT Policy ITP-B.8, "Security Education and Awareness," requires state agencies to provide information technology security education and awareness to employees and other agents of the state.
- 4.6 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

State agencies shall establish general password security policy in compliance with this state policy and ensure that all users adhere to that policy.

In addition, for applications designed to transact certain types of official state records electronically, as defined in Rule 123:3-1-01 of the Ohio Administrative Code, agencies shall apply more stringent password security. Refer to Rule 123:3-1-01 for more information on specific requirements for ***password length*** and ***password composition*** for e-government applications involving legally binding records or signatures.

Agencies shall define password policy based upon the results of the agency risk assessment in accordance with Ohio IT Policy ITP-B.1, "Information Security Framework." The policy shall comprise a combination of password factors: length, composition, aging, lockout and history. The combination of these factors affect the level of security associated with a password. For example, a common recommended configuration of password factors for systems requiring secured access is:

- Password Length: a minimum of eight characters
- Password Composition: a combination of alpha, numeric and special characters
- ***Password Aging:*** a maximum password life of 90 days
- Password History: a password cannot be reused within one year
- Password Lock-Out: a security action is taken after five password attempts

Agency password security policy shall include the following elements:

- 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 used 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. Agencies 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, agencies shall establish 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. The agency 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. A user account for a state controlled system 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. Passwords within those files shall be stored in a one-way encrypted or hashed form and not in plain text.
- 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 the state 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 the termination date. Passwords associated with involuntary terminations shall be deactivated immediately upon notification. The user's account may be maintained in the authentication database until all files owned by the user have been handled appropriately; at that time the user account should be deleted.

- 5.12 Compromised Passwords. Passwords compromised maliciously or by accident shall be deactivated immediately. All instances of maliciously compromised passwords shall be reported immediately in accordance with the agency's security incident reporting policy as defined in Ohio IT Policy ITP-B.7, "Security Incident Response."
- 5.13 Save Password Option. Agencies shall avoid system and application configurations that allow 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. Agencies 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 Password Distribution. State agencies shall ensure that the distribution of passwords maintains confidentiality, integrity and availability. Passwords shall be permitted only for authorized users pursuant to Ohio IT Policy ITP-B.1, "Information Security Framework Policy."
- 5.17 Education and Awareness. Agencies shall establish password management education and awareness efforts in accordance with Ohio IT Policy ITP-B.8, "Security Education and Awareness." At a minimum, agencies shall ensure the following is addressed:
 - 5.17.1 Password protection is the responsibility of each user.

5.17.2 Personal information such as social security number, meaningful dates, nicknames or other obvious information shall not constitute a password.

5.17.3 A review of agency policies on password composition.

5.18 Password Testing. Agencies shall configure systems to test password effectiveness regularly if that capability is available. Password testing should be conducted by authorized personnel only and should occur at least annually. Password testing should be conducted more frequently if deemed necessary by the risk assessment defined in Ohio IT Policy ITP-B.1, "Information Security Framework."

5.19 Default Passwords. Default application and system passwords shall be reset before deployment of any system or application. This requirement shall apply not only to conventional desktops, servers and notebook computers, but also to passwords for embedded systems, including network routers, switches and some networkable printers.

6.0 Procedures

None.

7.0 Implementation

The following additions to this policy resulting from the March 2008 revision shall be implemented by state agencies within six months of the effective date of this policy:

- Section 5.9, concerning password storage
- Section 5.11, concerning password deactivation
- Section 5.17 concerning education and awareness
- Section 5.19, concerning default passwords

The remainder of this policy continues in effect.

8.0 Revision History

Date	Description of Change
12/05/2002	Original policy.
12/05/2007	Scheduled policy review.
03/19/2008	Requirements concerning password and PIN management controls added to sections 5.9, 5.11, 5.17 and 5.19.
03/19/2013	Scheduled policy review.

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 information technology 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. 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:

Statewide IT Policy
Investment and Governance Division
Ohio Office of Information Technology
30 East Broad Street, 39th Floor
Columbus, Ohio 43215

Telephone: 614-644-9352
Facsimile: 614-644-9152
E-mail: State.ITPolicy.Manager@oit.ohio.gov

Ohio IT Policy can be found on the Internet at www.ohio.gov/itp.

12.0 Attachments

- 12.1 Attachment 1 – Interrelationship of the Information Security Framework Policy and Subpolicies. A cross-reference table showing the relationship between the primary framework policy and the subpolicies.

Attachment 1

**Interrelationship of the Information Security Framework Policy
and Subpolicies**

Information Security Framework	Security Requirements								
	Risk Management	Confidentiality	Integrity	Availability	Protect, Detect and Respond	Identification & Authentication	Access Control & Authorization	Security Audit Logging	Security Management & Administration
Information Security Framework Policy Sections	5.1	5.2	5.2	5.2	5.3	5.4	5.5	5.6	5.7
SUBPOLICIES									
Boundary Security (B.2)	X			X	X	X	X	X	X
Business Resumption Planning (E.7)	X			X	X				X
Data Classification (B.11)	X	X	X	X	X	X	X	X	X
Disposal, Servicing and Transfer of IT Equipment (E.1)	X	X							X
Internet Security (B.6)	X					X	X		X
Intrusion Prevention and Detection (B.12)	X		X		X		X	X	X
Malicious Code Security (B.4)	X		X		X				X
Password & PIN Security (B.3)	X	X			X	X	X	X	X
Portable Computing Security (B.9)	X	X				X	X	X	X
Remote Access Security (B.5)	X	X		X		X	X	X	X
Security Education and Awareness (B.8)	X	X	X	X	X	X	X	X	X
Security Incident Response (B.7)	X		X	X	X			X	X
Security Notifications (B.10)	X	X			X	X	X		X