



INFORMATION SECURITY AND PRIVACY POLICY

PASSWORD – PERSONAL IDENTIFICATION NUMBER

IT POLICY NUMBER: 2100-01

EFFECTIVE DATE: 12/05/2012

APPROVED BY:

Robert Blair, Director
Department of Administrative Services

1.0 PURPOSE

This policy addresses the use, management, and control of passwords and personal identification numbers (PIN's) used to access IT resources owned, managed, or operated by the Department of Administrative Services (DAS). References in this policy to passwords also apply to PIN's, except where explicitly noted.

2.0 SCOPE

The scope of this policy includes all accounts (or any forms of access that support or require a password) on any system that resides at any DAS facility, has access to DAS owned or operated networks, or stores any non-public DAS information.

This policy applies to computer and telecommunications systems owned or operated by DAS and the managers of DAS business units and IT systems that use or administer such systems.

3.0 BACKGROUND

A critical line of defense in computer system security is the user (i.e. anyone having authorized access to computer systems) and the password associated with that user. Passwords are the front line of protection for user accounts. Breach of user passwords is one of the easiest methods of gaining unauthorized access to sensitive information and systems. A poorly chosen password may result in the compromise of an entire network. Proper password management is an effective, cost effective and necessary measure in restricting unauthorized access.

DAS managers shall consider the guidance within the National Institute of Standards and Technology (NIST) Special Publication 800-53, revision 3 (NIST 800-53) for additional guidance to ensure systems are protected to an acceptable level.

4.0 REFERENCES

- 4.1. **Ohio IT Standard; ITS-SEC-02; Security Controls Framework:** This state IT standard specifies the minimum requirements for information security in all **agencies** and identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53, revision 3 (NIST 800-53) as the framework for information security controls implementation for the state.
- 4.2. NIST Special Publication 800-53 (Rev 3), *Recommended Security Controls for Federal Information Systems and Organizations*, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.
- 4.3. A glossary of terms found in this policy is included in Section **8.0 – Definitions**.

5.0 POLICY

DAS is issuing this policy to ensure compliance with related state policies and to protect DAS' IT resources. More detailed security standards and procedures supporting the implementation of this policy will be maintained separately.

The password policy for DAS encompasses a combination of password factors to ensure a minimum level of security is provided by password controls.

5.1 Requirements

- 5.1.1. The use, management, and control of passwords used to access IT resources owned, managed, or operated by DAS must conform to DAS' standards for password composition, length, aging, system lockout, history, issuance, storage, distribution, and transmission.
- 5.1.2. Uniqueness - The combination of user-ID and password shall authenticate a unique user. User accounts for DAS owned or controlled systems will be associated with a single individual and shall not be established for use by more than one person.
- 5.1.3. 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 termination date. Passwords associated with involuntary terminations shall be deactivated immediately upon notification.
- 5.1.4. Compromised Passwords - Passwords compromised maliciously or by accident shall be deactivated immediately. All instances of maliciously compromised

passwords must be immediately reported in accordance with DAS' incident response procedure.

- 5.1.5. Save Password Option – DAS shall avoid system and application configurations that allow for the use of save password options. When possible, any save password options shall be disabled at the system level. If a system's save password feature cannot be disabled, users shall be instructed not to use that option.

- 5.1.6. Administrative Accounts

DAS 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.

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

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. Programs 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, as these features become available.

- 5.1.7. Display - Passwords shall be hidden from display at all times. This includes both electronic and written formats and requires that any password input into a system is masked on-screen.
- 5.1.8. Training - All users must be instructed that the protection of passwords is the responsibility of each user and that they must maintain the appropriate safeguards to keep their passwords confidential.
- 5.1.9. Password Testing - DAS shall configure systems to regularly test password effectiveness. This includes the use of password cracking or guessing that may be performed on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Password testing should be conducted by authorized personnel only and should occur at a minimum semi-annually. Password testing should be conducted more frequently if deemed necessary to protect higher risk system assets.

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

6.0 RELATED PROCEDURES

DAS Procedure: Incident Response

DAS Procedure: Issuance of Passwords and PIN's

DAS Procedure: Privileged Account Password Compliance

Additional standards and procedures shall be developed at various levels within the DAS organization in order to effectively and efficiently implement this policy.

At a minimum:

- This policy shall be distributed to each newly hired DAS employee during orientation, in conjunction with other applicable policies and procedures, and the new employee shall sign an acknowledgement of receipt of this policy.
- Vendors, contractors, and temporary employees shall receive a copy of and sign an acknowledgement of receipt of this policy prior to gaining access to IT resources.

7.0 COMPLIANCE

It is the responsibility of management to implement and ensure compliance with the laws, rules, policies, procedures, standards, and license agreements applicable to the use of IT resources within their functional areas.

8.0 DEFINITIONS

DAS – Department of Administrative Services.

DAS Contractors – For the purposes of this policy, DAS contractors are defined as contracted staff and vendor technicians.

DAS Employees – For the purposes of this policy, DAS employees are defined as all employees and representatives of DAS, whether they are permanent staff or temporary staff.

DAS-owned – Purchased with DAS funds or otherwise acquired by DAS; property of DAS.

DAS-provided or DAS-supplied – Made available to users by DAS.

IT Resources – Any information technology resources, such as computer hardware and software, IT services, telecommunications equipment and services, networks, digital devices such as digital copiers and facsimile machines, supplies, and the Internet.

Management – Management refers to supervisory staff responsible for the completion of activities to fulfill DAS' mission. If Position A is shown as subordinate to Position B on the Table of Organization, then Position B is supervisory in nature for the purposes of this policy.

OIT – Office of Information Technology.

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.

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

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

Privately-owned - Purchased with personal or corporate (vendor or contractor) funds; not provided by the state.

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.

State-owned - Purchased with state funds or otherwise acquired by the state; property of the state of Ohio.

System Assets - System assets include information, hardware, software and services required to support the business of DAS.

Users - For the purposes of this policy, users are defined as employees, contractors, temporary personnel and other agents of the state who administer or use privately-owned (if authorized) or state-owned IT Resources on behalf of the state.

9.0 INQUIRIES

For information regarding this policy, please contact:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, Suite 4083
Columbus, Ohio 43215
Telephone: 614.644.9391
Email: state.isp@oit.ohio.gov
Web: infosec.ohio.gov

Department of Administrative Services policies can be found online at:

<http://das.ohio.gov/Divisions/DirectorsOffice/EmployeeServices/DASpolicies/tabid/463/Default.aspx>

10.0 REVISION HISTORY

Date	Description
12/01/2009	New policy for DAS, replaces OIT policy dated 6/29/07
12/05/2012	Policy reissued under Director Robert Blair.

11.0 ATTACHMENTS

Password PIN Exemption/Deferment Request