



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

Standard ID:	SE-PWD-001
Title:	Strong Password Authentication
Domain:	Security
Discipline:	Authentication
Revised Date:	07/11/2016
Revision no.:	7
Original date:	6/5/2006

I. Authority, Applicability, Purpose

- A. Authority:** Title 29, Chapter 90C provides broad statutory authority to the Department of Technology and Information to implement statewide and interagency technology solutions, policy, standards and guidelines for the State of Delaware's technology infrastructure. "Technology" means computing and telecommunications systems, their supporting infrastructure and interconnectivity used to acquire, transport, process, analyze, store and disseminate information or data electronically. The term "technology" includes systems and equipment associated with e-government and Internet initiatives.
- B. Applicability:** Applies to all State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies and standards promulgated by DTI as a condition of funding, access, and continued use of these resources.
- C. Purpose:** Authenticating users before they gain access to State information and resources has never been more important. Passwords ensure the security and confidentiality of such data, restricting access to only authorized staff. This standard defines the criteria for strong password authentication and applies immediately to any new application. Existing applications that contain full social security numbers are required to comply by 12/31/2014. All other existing systems must come into compliance at the next major system upgrade.

II. Scope

- A. State of Delaware:** All communications and computing resources.
- B. Areas Covered:** All information, resources, and solutions that require strong password authentication in accordance with Federal and State of Delaware policies and standards.
- C. Environments:** All environments such as operating systems, networks, applications, databases, etc. that require strong password authentication. Please consult current Federal and State of Delaware policies and standards for reference.

These standards are adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC), and are applicable to all Information Technology use throughout the State of Delaware. Any questions or comments should be directed to dti_tasc@state.de.us.



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

III. Process

- A. **Adoption:** These standards have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the State of Delaware.
- B. **Revision:** Technology is constantly evolving; therefore, the standards will need to be regularly reviewed. It is the intent of the TASC to review this standard annually. TASC is open to suggestions and comments from knowledgeable individuals within the State, although we ask that they be channeled through your Information Resource Manager (IRM).
- C. **Contractors and Vendors:** Contractors, vendors and other third parties are required to comply with these standards when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection by the Delaware Technology Investment Council. For further guidance, or to seek review of a component that is not rated below, contact TASC at dti_tasc@state.de.us.
- D. **Implementation responsibility:** DTI and/or the organization's technical staff will implement these best practices during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.
- E. **Enforcement:** DTI will enforce these best practices during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. These best practices may also be enforced by others during the course of their normal business activities, including audits and design reviews.
- F. **Contact us:** Any questions or comments should be directed to dti_tasc@state.de.us.



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

IV. Definitions/Declarations

A. Definitions:

1. **eGovernment Application** is an application that is designed for citizens or businesses to use from the Internet.
2. **SANS** is an abbreviation for 'SysAdmin, Audit, Networking, and Security'. The SANS Institute was established in 1989 as a cooperative research and education organization that provides information security training and certifications.
3. **Multi-factor Authentication** consists of a combination of two or more authentication methods. The State of Delaware currently uses RSA Keys. Multi-factor Authentication is to be reserved for those instances where strong passwords do not provide adequate security. Refer to the [Enterprise Standards and Policies](#) for further insight.
4. **Pass Phrases** are strings of words and characters typed to authenticate into a network as opposed to a password of usually 6 – 12 characters. Pass Phrases can be much longer, up to 100 characters or more.
5. **Resource Account** is a user account created to facilitate non-interactive authentication. Examples include Windows service accounts, Exchange resource accounts and accounts created exclusively for inter-device or inter-process communication.
6. **Service Account** is a user account that is created explicitly to provide a security context for services running on a Windows machine.

B. Declarations

This standard defines the criteria for strong password authentication.

This standard does not address passwords or pin numbers for mobile devices.

The password length for ACF2 passwords will remain at 8 characters until ACF2 is able to support 10 or more characters.

The ERP Portal is unable to comply, due to vendor (Oracle) restrictions, with the requirement to restrict password changes for a specific system to not more than once a day.



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

V. Definition of Ratings

COMPONENT RATING	USAGE NOTES
STANDARD – DTI offers internal support and/or has arranged for external vendor support as well (where applicable). DTI believes the component is robust and solidly positioned in its product life cycle.	These components can be used without explicit DTI approval for both <u>new projects</u> and <u>enhancement</u> of existing systems.
DECLINING – Deprecated - DTI considers the component to be a likely candidate to have support discontinued in the near future. A deprecated element is one becoming invalid or obsolete.	Via the State's waiver process, these components must be explicitly approved by DTI for <u>all projects</u> . They must not be used for <u>minor enhancement</u> and <u>system maintenance</u> without explicit DTI approval via the State's waiver process.
DISALLOWED – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered.	No waiver requests for new solutions with this component rating will be considered.

- A. **Missing Components**: No conclusions should be inferred if a specific component is not listed. Instead, contact TASC to obtain further information.



VI. Component Assessments

Authentication Password Criteria

The State selected a password-based authentication scheme that makes compromises between what is convenient for the user and what is difficult to circumvent. The scope of this standard includes all user credentials for all organizations including contractors who interact with, or handle State of Delaware data or interact with the State network. Servers, desktops, mobile devices, and especially laptops are to comply. Refer to the [Enterprise Standards and Policies](#) and notably to the [Delaware Information Security Policy](#) for further insight.

Multi-factor authentication consists of a combination of two or more authentication methods. Currently, the State's second factor of authentication is an Entrust key which changes every 60 seconds. Multi-factor authentication is to be reserved for those instances where strong passwords do not provide adequate security.

Passwords must not be stored in plain text.

Why use Strong Passwords?

The guidelines for strong passwords are established by the SANS Institute and recommended by the Microsoft Corporation and other leading Information Technology organizations. These guidelines are consistent with the password policies at most major government facilities.

- Sarbanes-Oxley requires a minimum of 8 characters, reset within 45 to 90 days.
- HIPAA requires that passwords be reset every 45 to 90 days.

Why use Pass Phrases?

- Studies suggest that users are more apt to remember a Pass Phrase than a long 12+ character password.
- The longer the Pass Phrase or Password the stronger they are and harder to compromise.
- Pass Phrases have the distinct advantage of higher entropy meaning a higher measure of randomness. Entropy consists of the number of items chosen, the size of the set from which they are chosen and the probability that each item is chosen as part of a Pass Phrase.



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

All passwords used to access State of Delaware data **must** adhere to the following characteristics for strong passwords:

- Passwords must be at least ten characters long. (The security of a password rises exponentially with the number of characters used in the password. Pass Phrases are recommended.)
- Active Directory (not K12) passwords (used for email, used for logging into Windows, etc) on the State network must be at least 10 characters long.
- A password must not be repeated within 8 resets.
- All personnel must treat passwords and other access credentials as confidential and should protect them from disclosure. Refer to the [Enterprise Standards and Policies](#) and notably to the [Delaware Information Security Policy](#) for further insight.
- Passwords must contain characters from at least three (3) of the following four (4) classes from the table below:

DESCRIPTION	EXAMPLES
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
English (Arabic) numerals	0, 1, 2, ... 9
English Non-alphanumeric ("special characters")	#, \$, %, & such as punctuation symbols etc.

All passwords used to access State of Delaware data except eGovernment applications **must** adhere to the following characteristics for strong passwords:

- A password for a specific system must not be changed more than once a day.
- Passwords must expire within 90 days. A shorter timeframe is encouraged.

All passwords used to access State of Delaware data **should** adhere to the following characteristics for strong passwords:

- Passwords should not contain your name or user name.
- Passwords should not be a common word or name.
- Should not repeat adjacent portions of a recently used password. (For example, first using a password like 'TooThbrush1', and then followed by 'toothpastE2'.)



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

All service/resource account passwords used to access State of Delaware data **must** adhere to the following characteristics for strong passwords:

- Passwords must be at least 32 characters long or the maximum number of characters available.
- Passwords must contain characters from at least three (3) of the following four (4) classes from the table below:

DESCRIPTION	EXAMPLES
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
English (Arabic) numerals	0, 1, 2, ... 9
English Non-alphanumeric ("special characters")	#, \$, %, & such as punctuation symbols etc.

A different service/resource account must be used for different services.

A named person must be designated as the owner of each service/resource account.