



DEPARTMENT OF ADMINISTRATION

Enterprise Policy

ETSS-ENTERPRISE PASSWORDS-2019

ENTERPRISE TECHNOLOGY STRATEGY AND SERVICES

Enterprise Password Policy

Date of Last Revision 03/10/2019

Brian Tardiff
(401) 462-1783
doa.entsec@doit.ri.gov

1. Purpose

- a. Establish policy for the effective implementation of strong password criteria to safeguard State of Rhode Island network resources.

2. Applicability

- a. This policy is applicable to all State of Rhode Island Executive Branch Departments¹ (including agencies, boards and commissions), its and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to State network resources, whether operated or maintained by the State or on behalf of the State. For this policy, the term "agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

- a. **Network Resources:** Information systems, system components, devices, and data that are accessible by computer via the local area network or State intranet. Network resources include:
 - (i.) Data, information, and files (in storage and intransmission).
 - (ii.) Desktop computers
 - (iii.) State issued mobile devices (e.g. laptops, tablets, notebooks, smartphones).
 - (iv.) Peripheral devices (e.g. printers, scanners, fax machines, monitors).
 - (v.) Licensed software, hardware, and network equipment (e.g. applications, phone systems, servers, routers, switches).
- b. **Brute Force Cracking:** A password guessing method where a computer attempts all possible password combinations until the password is guessed.

4. Procedures for Compliance

- a. **Password Length:** Passwords will be a minimum of 8 characters in length. In general, longer passwords are considered more secure as they are less likely to be guessed or brute force cracked.

¹ State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State Colleges, the General Treasurer, the Attorney General, or the Secretary of State.

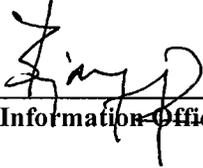
- b. Password Complexity:** Passwords will include at least one (1) character from three (3) of the following four (4) categories: uppercase letters (A, B, C ... Z), lowercase letters (a, b, c ... z), numbers (0, 1, 2 ... 9), and non-alphanumeric special characters([<\$@#& ...).
- c. Password Strength:** Passwords will not contain the user ID, email address, agency name or acronym easily associated with the agency, or dictionary words from any language. To effectively reduce the risk of unauthorized logical access to information systems, passwords should be complex enough to impede password cracking software tools, brute force attacks, and simple guessing of passwords. However, passwords that are too complex and cannot be remembered are not effective. An effective method for creating strong passwords is to use a passphrase (an acronym based on a sentence) that is easily remembered, such as a phrase, song, slogan, or quotation. For example, MsiS!Yold (my son is 5 years old) or lhliCfS#yN (I have lived in California for 5 years now). As a best practice, passwords used for State network resources should not mirror passwords used for personal accounts.
- d. Password Changes:** Passwords will be changed by the user at the initial account login and after a password reset. Passwords will not be identical to any of the previous twenty-four (24) passwords. The minimum lifetime restriction of passwords will be set to one (1) day. The information system will require that users change their account password at least once every ninety (90) days. Passwords for privileged accounts should be changed at least once every sixty (60) days or after a system administrator unlocks the account. Users requiring a password reset should contact the Enterprise Service Desk by phone (462-43 57) or email (ent.servicedesk@ri.gov) to create a service ticket request.
- e. Password Security:** Passwords will be encrypted when at rest and during transmission. Users will maintain the confidentiality of passwords and will not share their passwords with anyone. Users will promptly change their password whenever there is an actual or suspected password compromise or as directed by ETSS.

 - (i.)** The system administrator will disable the user account and notify the user immediately upon becoming aware of a compromised password. Passwords will be masked when being entered or presented on screen. Passwords should not be written on paper or stored in plaintext in digital format.
- f. Password Enforcement:** ETSS will enforce compliance with the requirements of this policy, whenever possible, via implementation of appropriate technical controls and methods (e.g. Active Directory Group Policy). If these requirements cannot be enforced for any reason, the agency will formally notify Enterprise Security in writing. The agency may be required to reimburse ETSS for financial costs associated with the implementation of operational and technical controls (e.g. hardware, software, dedicated personnel, overtime) necessary to mitigate consequences that result from unauthorized logical access to an information system that is not in compliance with this policy.
- g. Mobile Device Passwords:** Users will adhere to the guidelines of this policy when applying passwords to supervised mobile devices. Implementation of passwords on State issued smartphones will at a minimum, consist of a six (6) digit pin chosen by the authorized user. Biometrics, such as fingerprint or facial recognition is an authorized form of authentication for smartphones. When not in use, the user will lock the smartphone to enable pin / biometric authentication.

5. Repercussions for Noncompliance

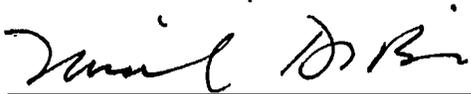
- a. Violation of the provisions of this policy will be subject to retraining, counseling and/or termination of access to network resources.

6. Signatures



Chief Information Officer

3/10/19
Date



Director of Administration

3/10/19
Date